A Location Privacy Model and Framework for Mobile Toy Computing

by

Laura Rafferty

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Computer Science

The Faculty of Business and Information Technology

University of Ontario Institute of Technology

August 2015

Abstract

Many toys on the market are becoming integrated with the sensory and networking capabilities of mobile technology. Toy computing is an emerging area of research with the characteristics of physical computing, services computing, mobile technologies, and Bring Your Own Device (BYOD). There is currently no standard privacy-preserving framework for mobile toy computing applications. Children's privacy is becoming a major concern for parents who wish to protect their children from potential harms related to the collection or misuse of their private data, particularly their location. This thesis provides an access control model for location privacy for children in the mobile toy computing environment. From this model we derive a policy specification language using XACML vocabulary with extensions for location privacy, as well as a technical framework to enforce the policies. Finally, the framework is tested through prototyping and case studies for proof of concept.

Acknowledgments

First and foremost I would like to extend my deepest and everlasting gratitude and admiration to my supervisor, Dr. Patrick Hung, who has provided endless support, insight, and inspiration throughout my graduate studies. It has been an absolute privilege to work with him and I am sincerely thankful for all of the opportunities and lessons he has given me.

I would also like to extend a great thanks to my examining committee, Dr. Marcelo Fantinato, Dr. Miguel Vargas Martin, Dr. Bill Kapralos, Dr. Kamen Kanev, and Dr. Andrew Hogue for their insightful suggestions and feedback for improving this thesis.

Thank you to Kevin Pang and Bryan Pham who have offered their expertise with Android development and JMEDS. As well as a special thanks to Brad Kroese who has been a great support and encouragement from the beginning.

Special thanks as well to Jessica Clarke and Melissa Picard for their ongoing kindness and assistance with graduate and international program coordination.

Lastly, I would like to thank my parents and grandparents for their loving support and encouragement throughout my academic career. This work is dedicated to them and my beautiful niece, Skye.

Contents

List of Figures

List of Tables

List of Symbols

Below is a list of symbols used for mathematical notations in this thesis.

Symbol	Meaning
$\subseteq$	Subset
$\in$	Element
R: A$\rightarrow$B	R is a relation from A to B
$\Rightarrow$	Implies
$\times$	Cartesian Product
$\wedge$	Logical AND
$\vee$	Logical OR
$\emptyset$	Empty set
$\cap$	Intersection
_	Anything
$\exists$	There Exists
$\forall$	For All

Chapter 1 **Introduction**

1.1 Introduction to Toy Industry

Toys have been a part of human existence for thousands of years, across every culture, being uncovered from as far back as ancient Egyptian times. A toy is an item or product intended for learning or play, which can have various benefits to childhood development. Toys can have a variety of purposes including education, leisure, and socialization. As such a substantial part of the human development, toys have continued to maintain a presence in the daily lives of billions of individuals of all ages. While primitive toys included rocks and pinecones, they soon progressed into dolls, stuffed animals and trains. As new ideas continue to develop to reflect the era and culture, it becomes evident that the toy is a product which has evolved along with humankind. It has become a marketable product which has blossomed into a multi-billion dollar industry.

Electronic toys have gained popularity, consisting of electronic parts with embedded systems. In the past few decades, electronic toys such as Speak & Spell, Tamagotchi, and Furby had become popular. More recently, sensors, and networking capabilities have introduced a variety of new possibilities for the toy industry. Toy companies have embraced modern technologies such as mobile devices into the design of their products, reshaping the concept of toys and education [1] through mobile applications and augmented reality.

Trends from Toy Fair 2014 indicated that the future of toys is augmented reality [2] [3], which uses technology to superimpose virtual world on top of reality. Augmented reality has also been noted to have a significant presence in the toy industry dating back to 2012 [4]. These trends continued into Toy Fair 2015 with RCs that interact with smartphones, apps that allow children to play with toys in new and different ways,

augmented reality and wearables [5]. Electronic toys have evolved to become more interactive and personalized to the individual user's preferences and environment by providing services which react to sensing technologies, and can create an augmented reality experience. The NPD's 2013 review of the Global Toy Market [6] identified the toy category of *youth electronics* as the most prominent subcategory of toys in terms of growth in the U.S. and Europe. This was also a trend identified at Toy Fair 2015 [5]. Further, Euromonitor International's research from 2015 [7] indicates that phenomenal growth in smartphones and tablets stimulate digital gaming, while electronic toys such as children's tablets and cross-platform toys such as amiibo have been a growing trend. In the U.S., the toy industry generates approximately $22 billion in annual retail toy sales, while the total economic impact of the toy industry in the U.S. is over $75 billion as of January 2015 [8]. Many countries have safety standards and regulations limiting the types of toys that can be sold on the market in order to protect the safety and privacy of customers.

Toy computing is a recently developing concept which transcends the traditional toy into a new area of computer research using mobile technologies. A toy in this context can be effectively considered a computing device or peripheral. Toy computing is comprised of two main topics in computer science: physical computing, and mobile services. Physical computing builds upon the traditional idea of the toy by bestowing it with potential embedded systems and sensory devices to create a more reactive and pervasive experience. Mobile devices act as the primary computing device and may also use sensors, while hosting mobile applications and services which complement the physical device. Physical computing combined with mobile services can create an augmented reality environment for toy computing through which users can immerse themselves in the toy computing experience. Augmented reality is the result of overlaying virtual components which react to real-world triggers captured through cameras and/or other sensors. This is achieved through the combination of physical computing with mobile services.

The toy may be endowed with sensory and/or networking capabilities, allowing for new opportunities for personalized services based on user preferences and environment. This introduces a Service Oriented Architecture (SOA) approach. One of the key concepts with this type of personalized services is contextual data. The application is able to gather data on the context of the user (e.g. time of day, location, weather) and provide personalized services based on this context data.

In modern times, with the proliferation of personal mobile devices such as smartphones and tablets, many service-oriented distributions have taken on a “bring-your-own-device” (BYOD) model. BYOD is an emerging application distribution model that encourages users to use their own mobile devices to access various online and mobile services. BYOD is being adopted by many traditional consumer electronics products such as electrical appliances and toys. Many studies found out that the traditional services enforcement mechanisms cannot cope with the complex security requirements of the emerging BYOD paradigm because the mobile devices are outside the infrastructure’s scope and control [9] [10]. Moreover, the mobile devices may run third-party services that could, intentionally or unintentionally, violate the safety policy. Most of the related solutions provide a mobile device management service that can block or even reset devices violating the security policy based on blacklist or whitelist approaches in place without advanced behavioral analysis such as motion sensing data in the mobile device. Some toys have become integrated into mobile devices, using apps, sensors and Near-field Communication (NFC). This introduces issues with trust which did not previously exist with traditional electronic toys, which operated on their own trusted platform. With the BYOD model comes additional concerns for privacy controls due to the introduction of an untrusted mobile device intended as the primary trusted system.

While toys become increasingly integrated with mobile devices, they also take on the privacy and security risks of such devices. Data that is collected to personalize the experience is also sensitive data that needs to be kept private from unwanted third parties. Information privacy is of great concern to many users who are becoming

increasingly worried about how their personal data is being collected and managed. Location data is particularly sensitive, as it can be used to infer a significant amount of private information about a user, such as movement and lifestyle patterns, workplace, etc. One of the major areas where toy computing differs from other types of mobile services is the user base. While users are primarily children or teenagers, privacy and security is an especially high priority. It is important to keep in mind the specific privacy concerns, laws and regulations for these users.

Privacy policies are a way of communicating to end users how their data is collected, managed, shared, and retained. However, the issue of policy enforcement remains an issue here. There is currently no standard framework in place for developers to follow for privacy preservation of mobile toy applications. This thesis aims to address this issue by introducing a formal access control framework for privacy preservation for mobile toy applications, with a focus particularly on location privacy. The framework is designed to allow users to define their own privacy preferences which will then be compared to a service's privacy policy before it is permitted access to their sensitive data. We provide a formal model for defining location, which we have adapted into an extended eXtensible Access Control Markup Language (XACML) [11] vocabulary with extended entities for defining location privacy specifications.

1.2 Motivation for Privacy

Although toy computing inherits the laws and regulations of its components, there is a unique need for this research particularly in the area of toy computing. While many of the same ideas can be adapted to other non-toy areas such as wearable devices, or even smartphone apps that use location-based services, this thesis focuses on the perspective of toy computing. Toy computing has unique requirements, including specific needs for children, as well as the relationship between the child, app, and physical toy component. There is no legislation or industry standard which specifically regulates privacy for toy computing. As a result, it is difficult for toy companies to have a basis for

how to best protect the privacy of users. From the consumer perspective, it also is a challenge for parents to manage the privacy of their children.

While the use of toy computing provides a unique source of entertainment, allowing children to express themselves, connect and communicate with their family and friends, there are several factors that contribute to the unique requirements for privacy in toy computing. The first factor is the user base, children under the age of 13. The personal data of children is widely considered to be especially sensitive and should be treated with extreme care [12] [13] to ensure their safety. Toy computing inherits the online safety threats of traditional online services which children can be vulnerable to including harassment, stalking, grooming[1], sexual abuse or exploitation, or personal data misuse [14]. Sexual solicitation and internet-initiated offline encounters are a major issue for the online safety of children [15]. The U.S. Department of Justice [16] indicates that "1 in 25 youths received an online sexual solicitation in which the solicitor tried to make offline contact." All of these risks are increased with the possibility of a potential solicitor becoming aware of the child's location or historical location patterns. On the other hand, children also take up a large segment of the consumer population and are of particular interest to market researchers who may attempt to collect their personal data and usage patterns for targeted advertising [17]. Third party advertisers can infer a great amount of information about a child based on their location and other context information, collecting detailed behavioral profiles that may be used for unknown or unwanted purposes.

Children are protected by international regulations such as the United Nations Convention on the Rights of the Child (CRC) [18], which protects children from all forms of violence, exploitation and abuse and discrimination, and ensures that the child's best interest should be the primary consideration in any matters affecting them. Information privacy laws such as the Personal Information Protection and Electronic Documents Act (PIPEDA) [19] in Canada have been developed to protect the online privacy of users,

[1] 'Grooming' is a term which refers to the process by which an individual befriends and interacts with a child online in attempt to persuade them to perform sexual acts [9].

including children. It is of great concern to parents that the toys and services which their children have access to comply with these privacy laws, for the safety and protection of their children. To our understanding, toy safety guidelines are out of date with the current innovations in toy technology. Toy safety guidelines such as Health Canada's Safety Requirements for Children's Toys and Related Products [20] concentrate on physical safety related to traditional toys and do not mention any restrictions related to privacy. These guidelines had been written to protect children's safety with electronic toys, however they have not expanded with recent developments in toy technologies which now have a wide range of sensory and networking capabilities creating new privacy risks. The unique environment of toy computing has exposed a need for unique privacy considerations which we aim to address in this thesis. For the purpose of this thesis, we focus on protecting the privacy of location data for children using toy computing devices. Location data is one of the most prominent forms of context data, as a significant amount of personal information can be inferred based on it.

1.2.1 Privacy Laws and Regulations

Privacy protection laws define the rights of data subjects (users), the responsibilities of data collectors (service providers), and methods for dispute resolution. These laws are generally enforced through ombudsmen (e.g. Privacy Commissioner of Canada), or licensing bureaus (e.g. CNIL in France) [21]. Different countries and legislations have different laws for privacy protection. These laws can also differ depending on what type of information is being collected (e.g. health information), or who the users are (e.g. children under the age of 13).

The Personal Information Protection and Electronic Documentation Act (PIPEDA) [19] is Canada's national privacy law which governs how personal information can be collected, used, and disclosed in commercial business. PIPEDA is based on the 10 principles of the Canadian Standards Association's Model Code for the Protection of Personal Information [22], which is recognized as a national standard in 1996. This model code is a representative of principles behind privacy legislation in many countries, including the

European Union. PIPEDA requires organizations to obtain consent when collecting, using or disclosing personal information, and to provide information regarding who is collecting the data, why it is being collected, and for what purpose it will be used. Personal information is defined in PIPEDA as "information about an identifiable individual, but does not include the name, title or business or telephone number of an employee of an organization." PIPEDA also allows individuals the right to see and correct any personal information about them collected by companies. Under PIPEDA, personal information can be collected about as long as it is:

- Gathered with the knowledge and consent of the person;
- Collected for a reasonable purpose;
- Used only for the reasons for which it was gathered;
- Accurate and up to date;
- Open for inspection and correction by the consumer; and
- Stored securely.

While PIPEDA requires meaningful consent for the collection of personal data collection, it does not refer to a particular age threshold for this. There is a difficulty in determining if a child is able to provide meaningful consent, as this greatly depends on their cognitive and emotional development and their understanding of privacy and online practices [12]. The Office of the Privacy Commissioner of Canada (OPC) has made the following recommendations regarding the management of the personal information of children and youth [12]:

- "Children's information is considered sensitive and merits special consideration under privacy laws."
- "Organizations should implement innovative ways of presenting privacy information to children and youth that take into account their cognitive and emotional development and life experience."

The United States Federal Trade Commission (FTC) has the Children's Online Privacy Protection Act (COPPA) [23] which protects the online privacy of children under the age of 13. COPPA indicates that a child's personal information cannot be collected without parental consent. In 2010, an amendment to COPPA further elaborated that personal information includes geolocation information, photographs, and videos. While Canada does not have an equivalent to COPPA, the OPC has indicated in the Online Behavioural Advertising Guidelines [24], a focus towards protecting children's online privacy particularly in the region of online behavioural targeted advertisements. The OPC recommends for organizations to avoid knowingly tracking children and Web sites aimed at children.

While technology continues to change, there are limitations on privacy laws and many countries and states struggle to keep up with the changing environment. Privacy related to location information, child users, and responsible marketing to children have been emerging topics in recent years. In order to help regulate this, several regulating organizations have provided guidelines and recommendations for industry *self-regulation* of the management of children's data online and mobile environments. The International Telecommunication Union (ITU) and United Nations Children's Fund (UNICEF) have released guidelines for child online protection, stressing that companies in states which lack adequate legal frameworks for the protection of children's rights to privacy and freedom of expression should follow enhanced due diligence to ensure policies and practices are in line with international law [13]**.** The guidelines encourage companies to adopt the highest privacy standards when it comes to collecting, processing and storing data from or about children [13]. Further, services directed at or likely to attract a main audience of children must consider the risks posed to them by access to, or collection and use of, personal information (including location information), and ensure those risks are properly addressed [13].

1.3 Toy Computing Model

Toy computing is a configuration where the physical toy component interacts with a mobile device which connects to one or more mobile services to facilitate gameplay. Figure 1.1 presents a model of the toy computing environment for the purpose of this thesis. This model illustrates the interactions between the physical toy component and the mobile device, as well as the interaction between the mobile service and the mobile platform when the mobile service attempts to access location data resources. In this model we have three entities: the physical toy component, the mobile device (platform), and the mobile service.

The physical toy component is an item much like a traditional toy, and can take the form of anything such as a doll, block, ball, or blaster. The toy interacts with the mobile device through one or more types of interactions. The types of interactions a toy can have with the mobile device include physical interaction by touching a button or screen, visual interaction as detected through a camera on the mobile device, audible interaction as detected through a microphone on the mobile device, or through network interactions such as Bluetooth, RFID or Wi-Fi. The physical toy component may also have sensors which collect and send sensory data to the mobile device.

The mobile component of the model includes the mobile platform, location resources, and the mobile service. The mobile platform facilitates access restrictions between the mobile service and the resources located on the mobile device. Location data is often used by mobile services to provide relevant location-based services to a user. In a toy computing environment, location data can be used to locate other players. Location data is in the form of Global Positioning System (GPS) coordinates, latitude and longitude, to indicate the physical location of the device. Location accuracy can be expressed as fine or coarse, depending on the method it is collected.

This model incorporates the BYOD *Walled Garden* concept as outlined by the Whitehouse [25], to contain data or application processing within a secure application on the personal device so that it is segregated from personal data. As depicted in Figure

1.1, the mobile service is within a Walled Garden. A Walled Garden in a BYOD environment provides a trusted platform which can make access control decisions based on policies.

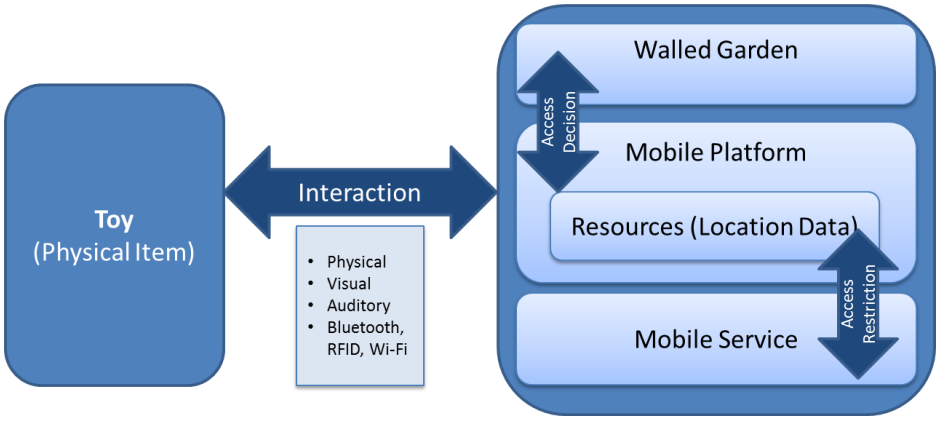

Figure 1.1 Toy Computing Environment

Referring to the three types of context data as defined by the World Economic Forum [26] (further described in Chapter 2), context data can be volunteered, observed, or inferred. During the course of the interactions between the toy and the mobile device, we are concerned with preserving the privacy of observed location data. Location data is observed as it is not explicitly provided by the user, but rather it is detected through the GPS sensors located on the mobile device. Figure 1.2 shows a GPS location (latitude and longitude) on a mobile device using the popular application Google Maps. Location data will be represented through latitude and longitude, and time.

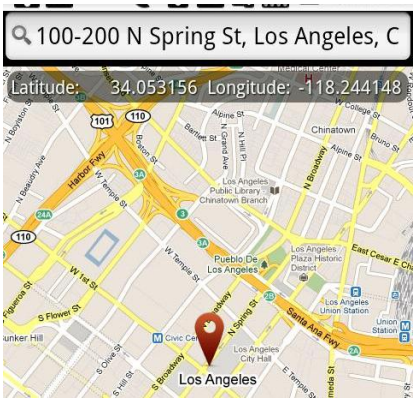

Figure 1.2 GPS location on a mobile device using Google Maps. Adapted from play.google.com

For the purpose of this thesis, a session is the duration of a game. The duration of a game starts with the interaction of the toy with the mobile device. The access to the location resources will be determined when the game starts, and end when the game finishes. Figure 1.3 depicts the concept of a session between a user and the toy computing system, comprised of the physical toy, and a mobile device running a mobile service.

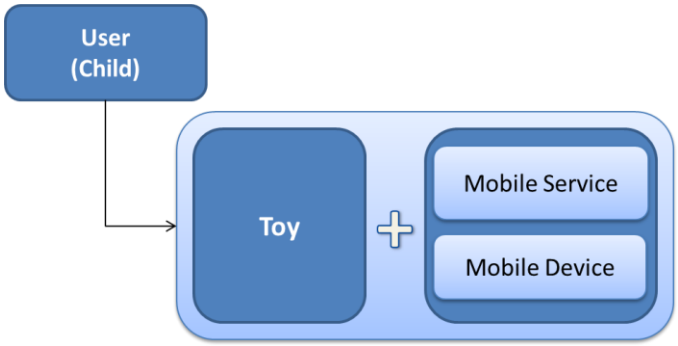

Figure 1.3 User and Toy Computing System

1.4 Contributions

The main contributions of this thesis are summarized as follows:

1. To define the concept of toy computing as an emerging research area.
2. To identify the unique location privacy requirements for toy computing.
3. To present a privacy access control model for location data in toy computing.
4. To present a novel technical framework for preserving location privacy in toy computing, including:
    - An extended XACML vocabulary for location privacy.
    - Technical framework to enforce the policies.
    - Prototyping and case studies for proof of concept.

1.5 Thesis Organization

This thesis is organized into six main chapters. This first chapter provides an introduction to the thesis, with an overview of the content and motivation. This is expanded upon in Chapter 2 with a comprehensive background on toy computing and related topics

including physical computing and mobile services technologies. Chapter 2 includes a discussion of some current toy computing products on the market, as well as a technical background on related technologies, an overview of access control and privacy concepts and a discussion of related works in this research area.

Chapter 3 establishes the privacy requirements for location data in a mobile toy computing environment. This chapter uses privacy threat modeling techniques and investigates current laws and regulations which apply to this context, particularly related to users who are children and their parents who wish to employ privacy controls to protect their privacy. From these requirements we present six privacy constraints.

Based on the privacy requirements outlined in the preceding chapter, Chapter 4 presents a privacy access control model for location data in toy computing. In this chapter we adapt core access control techniques and combine them with privacy-based entities. We define how the model addresses the six constraints based on the privacy requirements outlined in Chapter 3, and present an algorithm for access control decisions for privacy enforcement.

Chapter 5 establishes a novel location privacy enforcement framework for toy computing. This chapter presents an extended XACML vocabulary for location privacy adapted from the access control model in Chapter 4. The chapter defines the framework's request and response process, and algorithms for policy decisions. This chapter also presents a prototype implementation of the framework to enforce privacy preferences of the user, and includes case studies as proof of concept. Lastly, the thesis is concluded in Chapter 6 with some discussion on limitations, potential future works, and some concluding remarks.

Chapter 2 **Background**

The purpose of this chapter is to provide a background on the fundamental concepts of Toy Computing, including mobile services, physical computing, and augmented reality. It will also present some examples of toy computing products currently on the market. The chapter will also provide a background on security and privacy and relevant research works on these topics in order to provide the necessary foundations for the rest of the thesis.

2.1 Toy Computing Background

2.1.1 What is Toy Computing?

Mobile devices have become prevalent in many aspects of our daily lives. The reason for this is the portability and flexibility of the devices which can easily support applications developed for a wide range of uses. More recently, another use for mobile devices has been introduced in the area of toys and gaming. Toy companies such as Hasbro, Mattel, and Tech4Kids have released toys that integrate with mobile platforms, providing new capabilities and add-ons to traditional functionality [27]. These have been referred to as *Augmented* [28], *Interactive* [29], or *Smart Toys* [30], because they include sensory capabilities to allow them to detect and interact with their environment. Related fields include physical computing, mobile services, context and location-based services, and augmented reality. At its most basic level, a toy computing system can be identified as a toy equipped with sensory technology, mobile computing power, and communication capabilities [28]. This differs from a traditional electronic toy in how it incorporates a mobile component, whereas traditional electronic toys are isolated to their own proprietary platform. For the purpose of this thesis, the two basic components that make up a toy computing system include a) the physical component, which is similar to a traditional toy, and b) the mobile component, a smartphone or tablet running an application to provide services to the user/toy.

The physical component of a toy computing system observes almost the same overall characteristics as a traditional toy, with the potential addition of embedded systems, networking capabilities or sensors designed to communicate in some way with the mobile component. This physical component can take the form of any traditional toy, such as a blaster [31], block [32], or stuffed animal [33]. The physical component may or may not contain embedded systems or networking capabilities; however it must be able to interact in some way with the mobile component. An interaction can be physical, visual, auditory, or through networking such as Bluetooth, RFID or Wi-Fi.

In this configuration, the mobile device takes on the position as the primary computing device of the system. This includes the CPU, memory, sensory input, and output. The mobile component will run an application which operates in collaboration with the physical component to provide services to the user based on their interactions with the physical component. For the purpose of this thesis, we will be concentrating on *Toy Computing* from a mobile services perspective. There is a multitude of built-in sensory capabilities on mobile devices, which provide a new wave of opportunities for human computer interaction and personalized context-aware services. Depending on the toy, the sensory capabilities may either be located on the physical component, the mobile component, or both. Figure 2.1 illustrates the relationship between physical computing and mobile services to form a toy computing environment.

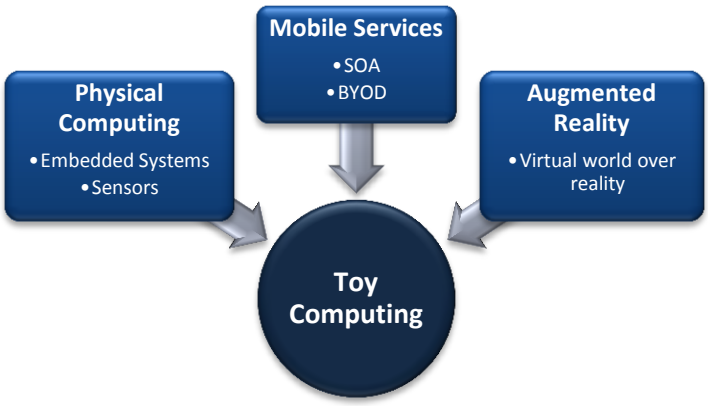

Figure 2.1 Toy Computing Components

2.1.1.1 Examples of Toy Computing Products

Toy computing is quickly gaining popularity in the toy industry. These toys have a wide variety of categories including toy blasters, language blocks for educational purposes, and methods of communication for children. Below are some examples of popular toy computing products currently on the market.

Tek Recon

Figure 2.2 Tek Recon "Havoc" blaster with mobile device mount. Adapted from www.tekrecon.com

Tek Tecon [31] is a line of toy blasters developed by Tech4Kids, marketed to children aged 8 years and up in 2013. While this product features a physical component identical in concept to a traditional toy blaster, the novelty is the ability to integrate with a mobile device. Referring to Figure 2.2, the Tek Recon blaster features a mount on top where a smartphone is inserted. A mobile application has been developed by Tech4Kids which operates in collaboration with the physical blaster to augment traditional blaster-based games. The application provides several functionalities including a scope, which uses the smartphone camera to display what is in front of the user with additional features overlaid on top, such as ammunition, score, radio, and a GPS location map of other players. The application has networking functionality to create and join games with friends over a LAN or mobile network. The user is also required to create an account online, where the scores and account information are stored.

Sphero

Figure 2.3 Sphero robotic ball. Adapted from www.thinkgeek.com

Another recent toy computing product in the industry is Sphero [34], first introduced in 2011 by Orbotix, which then released subsequent versions, Sphero 2.0 in 2013 and Sphero Ollie in 2014. Referring to Figure 2.3, Sphero is a robotic ball which can be controlled and programmed through the user's smartphone or tablet. There are over 30 apps available for Sphero, most of which are games, while others are focused on education. This product is marketed not only to children and can be appropriate for any age group. While the physical ball component is a very simple and traditional concept, the capabilities of the toy increase substantially with the inclusion of robotics and a mobile device. The Sphero ball has wireless networking capabilities, an accelerometer and gyroscope, rolls in every direction, and glows different colors. Sphero can be programmed by the user through an app called Sphero Macrolab, which includes a set of predefined macros, and more advanced users can use another app called orbBasic to program in a language based on BASIC.

ChineseCUBES

Figure 2.4 ChineseCUBES. Adapted from www.chinesecubes.com

ChineseCUBES [32] is a toy computing product first introduced in 2011 which combines augmented reality technology with physical blocks to help the user to learn Chinese characters. Referring to Figure 2.4, the AR markers on the cubes are arranged in a certain order and detected by the webcam to create an interactive audio/visual experience with the software on the computer or mobile device. The software includes multiple features such as interactive stories, lessons and videos. The compute or mobile device does all of the sensing and processing in this scenario, and the physical cube components are entirely traditional.

Toy Mail

Figure 2.5 Toy Mail character, "Snort." Adapted from www.toymail.co

Toy Mail [35] is a toy introduced in 2013 which can connect to the user's home WiFi network and interact with the free Toy Mail mobile app. Once the app is installed on a mobile device, the user can record a message which will be sent to the toy. When a

message is received, the toy (as shown in Figure 2.5) will make a snort, wheeze, or whine sound to let the user know that they have received a message, which can then be played and replied to.

Other

Toy computing has been also been developed for a wide range of purposes such as language learning [36], early childhood education, and for children with ADHD and autism. For example, Auti is a socially assistive robotic toy which encourages physical and verbal interactions in children with autism [37]. Educational toys such as roBlocks and SmartTile encourage children to learn about robotics and programming while they play [38]. There has also been research on monitoring children's developmental progress using augmented toys and activity recognition [39].

2.1.1.2 Design Guidelines for Toy Computing

Hinske et al. [40] provide a Summary of Design Guidelines for Integrating Pervasive Computing Technology into (Traditional) Toys:

1. The technological enhancement must have an added value.
2. Specify what actions/tasks are to be supported.
3. Let the focus remain on the toy and the interaction itself, not the technology.
4. Integrate the technology in such a way that it is unobtrusive, if not completely invisible.
5. Toys should be still usable (in the "traditional" way) even if the technology is switched off or not working.
6. Tightly intertwine design and implementation
7. The technology should be reliable, durable, and safe.
8. Offer immediate and continuous feedback.
9. The added technology should support the high dynamics of play environments.
10. Employ an iterative development process, including rapid prototyping and testing.

The above guidelines reinforce that the integration of pervasive computing technology (i.e. in the context of toy computing) should provide added value and seamless integration with the physical toy component. Further, the technology should be reliable, durable, and safe. From the perspective of privacy, this introduces a need for a privacy preserving framework which protects the child from privacy threats while not taking away from the play experience by introducing obtrusive policies.

2.1.2 Physical Computing

Physical computing is a branch of computing which involves the integration of computing technology into a physical device which interacts with its environment. This is similar to the concept pervasive or ubiquitous computing, in which the computing device establishes itself into the users' daily physical activities. A pervasive computing environment is an information-enhanced physical space, not a virtual environment that exists to store and run software [41]; where the design of the system takes a human body as a given, and attempt to design within the limits of its expression [42].

The distinction between physical and pervasive computing is that physical computing has more of a focus on the physical objects involved rather than completely seamless interaction. In toy computing the physical toy component is an active part of the user experience, whereas in pervasive computing there would be little to no physical component and the system works seamlessly with everyday activities. One of the main characteristics of both pervasive and physical computing devices is its ability to perceive context information on the surrounding environment in order to react accordingly [41]. This perception is done through sensors on the device such as a microphone, camera, or accelerometer. Perception of this context information is fundamental to the device's ability to make timely and context-sensitive decisions.

As mentioned previously, the physical component of the toy computing environment would be the traditional toy itself, which will be complemented with embedded systems or sensor technology which communicates with the mobile application. In this system, personalized services are provided to the user based on context data collected and

inferred through sensors and other environment data. With the pervasiveness of modern mobile devices, vast amounts of information can be collected and inferred about the user and their environment. Physical computing often involves a networked environment, which introduces privacy and security issues, particularly related to the context information the devices are processing. While the toy is the physical component in this system, the mobile device is what provides computing functionality and sensory perception, as described in the next section.

Figure 2.6 Sphero robotic ball as a physical toy component. Adapted from www.gosphero.com

Physical computing introduces physical objects as interface components. The examples in the previous section demonstrate this with a toy blaster, ball, and cubes, which are all used as an interface similar to a traditional toy, but with enhanced interactive capabilities. As seen in Figure 2.6, the Sphero robotic ball acts as the physical interface component in a physical, toy computing environment.

2.1.2.1 Sensors

Modern mobile devices are created with a variety of sensory capabilities. In a toy computing environment, developers may embed sensors into the physical toy component, or take advantage of sensors already built into the mobile device. Through these sensors, motion and other data can be detected in a number of ways. Sensors can be categorized into three different types: motion sensors, position sensors, and

environment sensors [43]. Below is an analysis on some of the different types of data that can be gathered from these sensors.

- **Motion Sensors**: Motions sensors capture the physical motions of a device. Mobile devices can include a number of sensors for measuring motion including an accelerometer, gyroscope, magnetometer, barometer, gravity, linear acceleration, and rotation vector. Motion is commonly represented through 6- or 9-axis sensor system (3-axis magnetometer, 3-axis gyroscope, 3-axis accelerometer). These types of sensors are commonly used for a variety of mobile applications such as games, as a way for the user to interact with the application (e.g. angling the device left or right to turn the character in a game). They have also been commonly used in fitness applications for tracking steps and calories lost during a walk, run, or jog. A popular example of this is *Zombies, Run!* [44], a mobile game application which takes motion sensor input while a user is running or jogging. The application provides missions for the user to complete by meeting certain fitness goals which correlate with the storyline.
- **Position Sensors**: Position sensors are also very popular in mobile systems. Some examples of these types of sensors include geomagnetic field sensor, proximity sensor, and GPS. Position sensors, particularly proximity and GPS, are very useful for mobile and toy computing due to the portability of mobile devices. Many applications use location-based services which use position sensors on the device to provide recommendations relevant to the location of the user. Some examples of this include Yelp [45], UrbanSpoon [46], which allow users to read and post reviews of nearby restaurants and other establishments. Other applications such as social media applications, Instagram [47] and Facebook [48], use position sensors to allow users to geotag their location along with their posts.
- **Environment Sensors**: Sometimes it is useful for an application to be able to detect data about the surrounding environment. While this is not used as widely as motion and position sensors in the mobile and toy computing environment, these sensors do have a lot of very useful applications in agriculture, health care, security systems,

aeronautics. Types of environment sensors include sensors for relative ambient humidity, luminance, ambient pressure, and ambient temperature. The most popular environment sensors in the context of a mobile environment are probably luminance and sound sensors. An example of an application that uses environment sensors is PressureNet [49], an Android application that measures atmospheric pressure using the atmospheric sensors built into most Android phones. Most smartphones use luminance sensors to adjust screen brightness based on lighting conditions.

2.1.2.2 Wireless Communication Technologies

While physical computing environment collects environment data through sensors, the data collected often needs to be communicated to a service provider or other devices over a wireless network. The service provider may be located on the user's mobile device, or another device on the local or wide-area network. Possible types of wireless communication technologies used in a mobile toy computing environment include: RFID, NFC, Bluetooth, WiFi, GSM, and UMTS/3GSM.

2.1.3 Context Data

Data observed and collected through sensors gather context on the user and their environment. Context is defined succinctly by Dey and Abowd [50] as "any information that can be used to characterize the situation of an entity." Schilit et al. [51] defined context as location, identities of nearby people and objects, and changes to those objects. Zimmermann et al. further categorized the elements for describing context information into five categories: individuality, activity, location, time, and relations. Individuality is personal information about a user, activity is data regarding physical activity, location is the GPS location, time is discrete time, and relations are inferences between two or more pieces of context data. In a context-aware system, services are provided to the user based on what is relevant to their context. Recent advances in mobile technology open up great opportunity for the collection and processing of context data in valuable ways. There are many types of private context data that can be

collected via a mobile application. The collection of this data allows applications to adapt to the user's environment and personalize services accordingly.

2.1.3.1 Types of Context Data

Mobile devices can capture a user's physical activity state (e.g. walking, standing, running, etc.) and store personalized information (e.g. location, activity patterns, etc.). This data is referred to as context data; data that is collected on the user and their environment. This data can be collected from sensors, provided explicitly by the user, or observed, such as the time of an event. Personal data can come in many forms including browsing history, friends list, and location information. Some other examples of relevant context information include [52]: Verbal context, roles of communication partners, goals of the communication/individuals, local environment, social environment (who is there), and physical and chemical environment. Information can be volunteered (e.g. profile data provided directly by the user) or observed (e.g. location data detected from GPS). Often, private information may seem trivial and not perceived as very sensitive to the user, while in practice it can actually reveal a large amount of personal information about them. The World Economic Forum [26] defines three types of context data, as categorized by the way it is collected: volunteered, observed, and inferred:

- **Volunteered Data**: data that is explicitly provided by the user. This can include personal profile information or preference settings.
- **Observed Data**: data not directly given by the user, but is detected by the device/application often through a sensor. Some examples of observed data include GPS location and time.
- **Inferred Data**: data deduced based on analysis of a combination of volunteered and/or observed data (e.g. where a user is likely to be going based on typical behavior). A lot can be interpreted on a user and their environment through inferences based on collected data. There is great value on this inferred data that would not be explicitly provided by the user.

Volunteered and observed data can be analyzed to infer significant amounts of personal information about the user. For example, forecasting trip destinations based on data from driving habits [53]. Collected data is the basis for many valuable context-aware services, which provide custom content or services to the user based on what is most likely to be useful to them.

2.1.3.2 Privacy Concerns

With all of this in mind, privacy is a growing concern among many users of mobile devices. While many users appreciate the value of targeted services, they still express concern over how their data is collected and managed without their knowledge. Cherubini et al. [54] identify privacy as a barrier to the adoption of mobile phone context services. 70% of consumers say it is important to know exactly what personal information is being collected and shared [55], while 92% of users expressed concern about applications collecting personal information without their consent [56]. Mobile applications have adapted countless services to better analyze context data and provide custom services that will bring the most value to a user based on what they are most likely to need.

While allowing context data to be collected for services can prove to be of great benefit to users, there is an ongoing tradeoff between utility and privacy [57]. In this physical mobile and pervasive environment, the timely delivery of services is fundamental. The amount of information collected often results in a tradeoff required between disclosing sensitive data and receiving context-aware services. In order to provide the most relevant services to the user, more personal and context information must be collected, which raises concerns of privacy. For example, a service can send special promotions and coupons to a user depending on what is most relevant to them. In order to provide the most relevant promotions, the service will need to collect certain context data such as their location, and also potential profile information such as age and gender to help to determine what their interests may be based on demographic. To gain even more context of the user, the application may collect and retain historical data on the user

such as previous movement patterns, to determine where they are likely to be at certain times, if they are travelling, or previous interactions with the application such as which promotions they had previously been interested in. In this example, it is clear that the more information is collected on the user, the more relevant services can be provided to them. However, the user may not be comfortable with the level of data that is collected and inferred on them. An application knowing where you are and what you are likely to be doing at any given time is likely to raise concern with users.

For this reason, context data is at the core of privacy concerns with many mobile applications. Privacy goals must be defined to ensure private data is managed responsibly. Further, detailed analysis is required to ensure that the user's sensitive behavior cannot be inferred based on collected data. There have been many solutions which aim to preserve the privacy of sensitive context data, as will be described further below. There are countless types of data that can be collected from a mobile device that must be considered when evaluating the scope of privacy. This is true of collected sensory data as described above, and also from within other applications, sensitive data can be collected such as a user's profile information, contact list, or calendar. All of this information can be collected and analyzed to determine context information about the user.

2.1.3.3 Location

Location data can be defined as data representing where a user is physically located. Location is one of the most prominent types of data for context-based services, existing as a key parameter to define context [58]. A user's location, combined with other context and historical data, can be used to infer an extensive amount of information including actions, speed, direction, and movement patterns. Location data can be collected from the device through GPS, WiFi, or mobile network satellite. It can also be inferred from other information such as IP address, although this can be inaccurate (e.g. in the case of a proxy).

Location is defined succinctly by Merriam-Webster [59] as “a place or position.” This definition has been extended by the National Geographic Encyclopedia [60] to establish three different types of representing location: absolute location, relative location, and type of location as follows:

- **Absolute Location** – the location expressed in a range or exact GPS coordinates of latitude and longitude. The absolute location can be expressed as coarse or fine; for example, an entire country, city, block, or exact coordinates.
- **Relative Location** – the location relative to another entity as a reference point; for example, a relative location can be expressed as the distance between User A and User B, or distance between User A and Device C, or User A and location D.
- **Type of location** – the location expressed in an assigned category. Some examples of this could be home, office, street, mall, or restaurant.

Generally, location is represented as a 3-dimensional vector of GPS coordinates (latitude, longitude), and altitude (optional). A location event also includes a timestamp. Android’s **GpsLocation** data structure represents the location of the device with the following data fields [1]:

- Size
- Flags
- Latitude
- Longitude
- Altitude
- Speed
- Bearing
- Accuracy
- Timestamp

Different ways of collecting location information can be more accurate than others. For example, there is GPS-based location (fine) or Network-based location (coarse) [61]:

- ACCESS_COARSE_LOCATION (Network-based) – allows and app to access approximate location derived only from network location sources (cell towers and Wi-Fi). This method varies in accuracy from 50 metres in urban areas, and several kilometres in rural areas with less cell tower coverage.
- ACCESS_FINE_LOCATION (GPS-based) – allows and app to access precise location from location sources such as cell towers and WiFi, and also the user’s GPS

coordinates provided from their device. Accuracy for fine location using GPS is fairly accurate from 2-20 metres.

While a huge number of mobile applications request access to user location data, this is one of the most sensitive types of context-data. The incredible amount of information that can be gathered from a user based on their location is immense. Whalen et al. [62] discuss some of the current privacy issues in mobile devices mainly focusing on the storing and transmitting of sensitive location based information over extended periods. This research states that a large amount of users do not even know that such information is being stored, and in some cases, still happens even if the user has explicitly restricted such data to be collected. This goes against the privacy principle of having the users consent before collecting this information. Another violation of privacy principles that is discussed in this paper is the amount of data that is being collected is much more plentiful, accurate, and goes on for a lot longer than it needs to. One of the causes of this disconnect is that most of the permissions for this information collection is buried in lengthy policies that users rarely read, and is enabled by default. It is very important to protect this information, having access to such information not only shows where we have been but it can be used to predict where we will be tomorrow, and that introduces a lot more security concerns. Patil et al. [63] go into further detail about the widespread usage of location data collection in mobile services and their interaction with social networking services. The paper details an online study on 362 participants to understand the preferences of users of location services. The majority of users expressed that their main incentive for using of these services was for social networking purposes. A number of users in this study (25%) also indicated that they have regretted sharing their location on at least one occasion.

Location privacy is a huge concern in the mobile and wireless environment. While it can appear trivial, location-based data can infer a lot of sensitive information about a user, including their activities, habits, interests, and personal relationships. Inference attacks are possible, such as knowing when a user will be somewhere based on movement

patterns and historical activity. This can potentially put a user at risk. Often, location-aware services do not require knowledge of the exact location, but rather, could provide just as valuable services with an approximation of the user's location [64].

These research works identify a great need for location privacy management and enforcement in mobile services. While toy computing has become a recent development in the union of mobile service and toys, research on safety and privacy guidelines for toy computing seems to have been largely overlooked. To the best of our knowledge, there is a gap in the research area of location privacy in the context of toy computing. First, there is no formal model for enforcing privacy or location privacy in particular, for children using such toys.

2.2 Mobile Services

Mobile devices, such as smartphones, tablets, and e-readers, have become increasingly popular in recent years, successfully integrating themselves into the lives of many users. A recent poll of 5000 people by TIME magazine reveals that 54% of respondents check their mobile device at least once an hour [65], while another study for GSMA shows that 68% of participants identified themselves as users of mobile internet/apps, with 38% of this subset considering themselves to be heavy users [56]. The immense popularity of these devices can be explained by their personal, portable, and pervasive nature. These characteristics create a unique platform for services, particularly those based on context data. Often, mobile devices will have one single primary user. The portability of a mobile device makes it possible for a user to carry it with them wherever they go, making it a highly personal device as well. Mobile devices are also designed to be easy and fast to use, and easily connect to networks, allowing the user to always stay connected to data and services.

Mobile devices use mobile services, which are services accessible through a mobile network. Mobile services, like Web services, use Service Oriented Architecture (SOA) as described in Section 2.2.3.1. Mobile services can be context-aware, gathering context information from the mobile device, and providing relevant personalized services based

on the context. To gather context information, a context-aware service can either listen for events sent by a context provider, or query the context provider. Gu et al. [66] propose a middleware for building context-aware mobile services, using a Service Locating Service to allow entities to locate different context providers. However, this model does not consider privacy preferences of the user.

2.2.1 Mobile Games and Location-Based Services

Location-based services, also known as location-aware mobile services, have become widely popular to provide information such as travel information, shopping, entertainment, and event information. Location-based services have been defined by Duri et al. [67] as "services in which the location of a person or an object is used to shape or focus the application or service." Pura [68] identifies location as one of the most promising applications of mobile commerce, due to the ability to allow service providers to offer customized services based on context and resulting in increased perceived value and loyalty of customers.

The mobile application industry has observed a widespread adoption of mobile game applications. This has been successful due to factors such as increased mobility and social network integration [69]. Location-based services have also been used in applications for games. The popular mobile game Angry Birds [70] has a location-based feature which allows users to compete with other based on a leader board associated with their location. MyTown [71] is another mobile game, reminiscent of Monopoly, where users can check in to a physical location, buy and sell properties, and collect rent from other players who check into the same location.

Kaasinen [72] conducted a study to investigate user needs for location-aware mobile services:

- Contents: topical up to date information, comprehensive relevant information, interaction (user is moving and can only provide limited interaction to device), push information based on both location and personalization, detailed search options, planning vs. spontaneity.

- Personalization: personal options and contents, user-generated content.
- Seamless service entities: consistency, seamless solutions to support the whole user activity.
- Privacy: the right to locate, use, store, and forward the location. Privacy requirements are based on legislation and social regulation. The paper also identifies P3P as a potential approach to manage user privacy preferences and compare them to the location-aware service's privacy practices.

2.2.2 Bring Your Own Device (BYOD)

Mobile services follow Bring *Your Own Device* (BYOD) architecture, meaning that the user has their own personal mobile device to run the service from. Mobile services thus need to be flexible and consider a variety of different devices. While the term BYOD is typically used to refer to employees bringing personal devices to a work environment, the same general idea is involved in any mobile services scenario. Mobile applications must operate in a controlled environment and must protect data and resources from other untrusted applications that may be running on the device. Further, the introduction of unregulated mobile devices onto a network can result in loss of control, data leaks, and potential network loss [9]. BYOD can introduce complications when it comes to investigation in the case of a security breach. This can be made simpler through thorough planning of policies and contracts indicating employee and employer (or in a more general case, user and service provider) rights [10].

A toy computing environment considers several properties of BYOD, although outside of a corporate environment. For the purpose of this thesis, we will be considering the following BYOD characteristics:

- The user's mobile device is untrusted.
- The mobile application is operating on top of this untrusted device.

The objective of BYOD is to isolate business applications from the rest of the system. This means isolation from other applications running on the personal device [73].

2.2.3 Mobile Service Architecture

Figure 2.7 illustrates a multi-layered model which illustrates the relationship between the conceptual, logical, and language layers of mobile services. This framework has been adapted from the Web services logical model presented by Hung et al. [74]. This model is an extension of traditional Service-Oriented Architecture to include layers for privacy-related access control, and also an End-Point Device Profile for mobile devices. Each layer will be discussed in the subsequent sections.

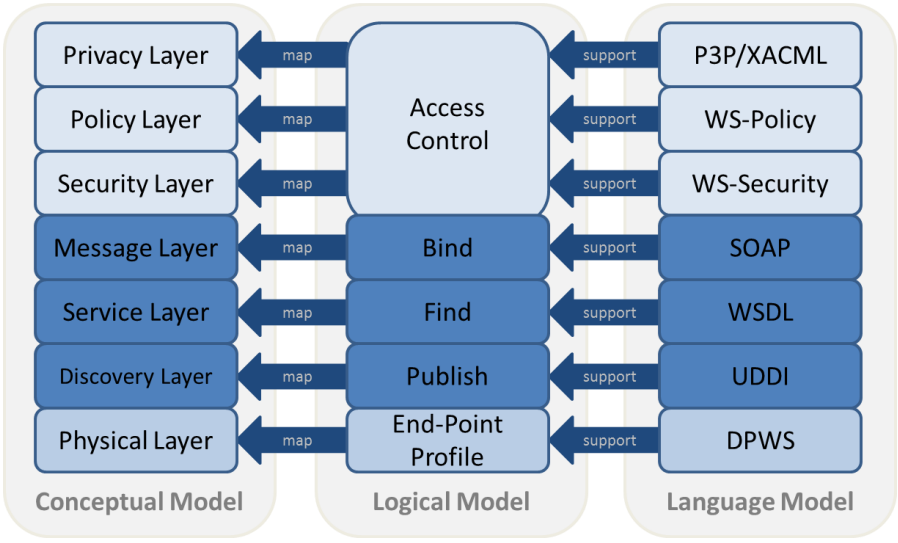

Figure 2.7 Mapping between different models and layers. Adapted from [74].

2.2.3.1 Service Oriented Architecture (SOA)

A theoretical model for Web services has been defined in Service Oriented Architecture (SOA). In our conceptual model, SOA consists of the message layer, service layer, and discovery layer. W3C defines SOA as a form of distributed systems architecture which typically maintains the following six properties [75]: (1) The architecture is defined in a *logical view*, in terms of what it does. (2) The *message orientation* property expresses how the service is defined in terms of the messages exchanged between provider and requester agents, rather than the internal architecture behind the provider's services. (3) *Description orientation* enforces that a service is described by machine-processable metadata. (4) SOA messages are also *granular* and (5) P*latform neutral*, meaning services tend to use a small number of operations with large and complex messages,

which are in a standardized platform-neutral format (ex. XML). Lastly, these services often tend to be oriented towards use over a *network*.

As seen in Figure 2.8, SOA consists of three entities: service provider, service requester, and service broker, and 3 operations: publish, find, and bind.

- **Discovery Layer (publish)**: In the model, the service provider will first "publish" details of its service (description and location) to the service broker, who saves it to the Universal Description Discovery Integration (UDDI) registry. UDDI is an OASIS standard which provides a directory of services available from each service provider.
- **Service Layer (find)**: The service requester queries the service broker with the "find" operation to find the service it is looking for, who will then return the details of the service. This layer uses Web Services Description Language (WSDL), an XML-based W3C standard for describing network services as a set of endpoints operating on messages [76].
- **Message Layer (bind)**: Finally, the requester uses the connection details to "bind" to the provider and receive services. The message layer uses Simple Object Access Protocol (SOAP), an XML-based protocol for request and response messages in web services.

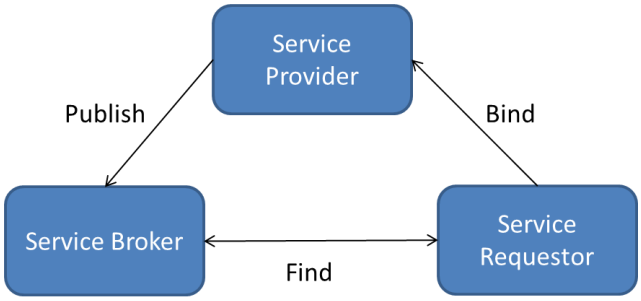

Figure 2.8 Service Oriented Architecture (SOA)

SOA is also been explored with mobile devices, with the mobile host acting as a service provider. The authors of [77] discuss the mobile host as a provider of services with SOA. It overviews the limitations with WS standards specifications on mobile cloud deployed services, as well as provide an architecture for supporting mobile clients in this

environment. It has not been demonstrated in a real-life environment yet, although they are working on deploying it on Amazon EC2. Service-Oriented Architecture for Devices (SOA4D) [78] is an open-source initiative aimed at the development of service-oriented software components (SOAP, WS-*, etc.) to fit the needs of embedded devices. SOA4D implements Device Profile for Web Service (DPWS), a specification designed for secure Web service communications on resource-constrained devices, as further described below.

2.2.3.2 Device Profile for Web Services (DPWS)

When software is running on any device, the application will need to communicate with other services whether they are internal or external (over a network). The Device Profile for Web Services (DPWS) [79] follows the SOA framework for automatic device and service discovery for networked embedded devices. DPWS offers a standardized device representation of services on a network and this allows for access to a set of built-in services such as secure accessing of metadata and exchange services by utilizing WS protocols. In other words, DPWS defines a minimal set of implementation constraints to enable secure Web service messaging, discovery, description, control, and eventing on resource-constrained endpoints [79]. The specification permits the definition of services for mobile devices considering the peer-to-peer direct communication between them that combine several devices as Service Oriented Architecture (SOA). DPWS allows sending secure messages to and from services, dynamically discovering a service, describing a service, subscribing to, and receiving events from a service.

In Web Services terms, a *profile* is a set of guidelines for how to use Web services technologies for a given purpose or application. Web services standards allow implementers to choose from a variety of message representations, text encodings, transport protocols, and other options, some of which are not interoperable. By constraining these decisions, profiles ensure that conforming implementations will work well together. DPWS is a profile developed by Microsoft and others for communication with and among networked devices and peripherals. The DPWS library for the .NET

Micro Framework is not a full Web services implementation but a lightweight subset with only the functionality needed to support DPWS on a device [80]. DPWS was built on the foundation of existing web services (WS) and as such uses many common specifications such as XML, SOAP, WS-*, WSDL and Message Transmission Optimization Mechanism (MTOM). DPWS defines two main types of services that are run by devices: hosting services, and hosted services [80]. Devices can be DPWS clients (invoking hosted services on devices), servers (providing hosting services), or both. DPWS for the .NET Micro Framework supports devices in either role or both simultaneously. Hosted services are the services that the device has, and depends on their hosting service for discovery. Hosting services allow other devices to use, subscribe and obtain metadata of the given services. DPWS defines the extensions required for using services in mobile devices, taking in account their specific constraints. A DPWS enabled device has access to provided functionality such as: the discovery of other, utilizing WSDL to describe a Web service, service subscription, and secure sending of messages, given that the other device also utilizes DPWS.

The Web Services for Devices (WS4D) [81] framework is an extension of DPWS to bring SOA and Web services technology to industrial automation, home entertainment, automotive systems and telecommunication systems. There have been ongoing initiatives to connect internet technologies and web services to resource-constrained devices in ad-hoc networks while conserving interoperability. WS4D provides technologies for easy setup and management of network-connected devices in distributed embedded systems [82]. Araujo and Siqueira [83] used WS4D to implement a DPWS Device Service Bus (DSB), establishing a Device Tunnel to deal with virtual devices and services.

Pohlsen et al. [84] present a plug-and-play architecture for connecting medical devices through DPWS, using WS-Discovery protocol. Unlike traditional Web service architectures, the authors propose using a WS-Discovery proxy server rather than a UDDI server, to better meet the requirements of resource constrained devices. Further,

the work uses SOAP-over-UDP (User Datagram Protocol) for multicast messaging, as included in DPWS. El Kaed et al. [85] present an implementation to interoperably connect Universal Plug and Play (UPnP) and DPWS smart home devices such as a TV, printer, and light bulb. DPWS does not support fine-grained security requirements, direct authentication between devices without a third party, and does not propose a comprehensive authorization concept [86]. All of these works present the foundation technologies for this research work. To the best of our knowledge, there is no unified framework for enforcement for location privacy in mobile services for toy computing.

2.3 Privacy and Access Control

2.3.1 Introduction to Privacy

When it comes to any information technology, privacy and security are at the core of ensuring that goals are achieved effectively and without compromise of personal data. The three concerns of security are confidentiality, integrity, and availability. Confidentiality means that access to information is restricted only to intended parties. Integrity means that data is accurate and consistent and has not been tampered with, while availability means that resources and data remain available when needed by the legitimate parties. A foundation of security is required for privacy.

Information privacy is defined by Hung and Cheng [87] as “an individual’s right to determine how, when, and to what extent information about the self will be released to another person or to an organization.” In particular, personally identifiable information is any type of information that can be linked to an individual, including their activities, preferences, history, conversations, etc. In a mobile environment, personally identifiable information is also likely to be gathered from context data, as described in the previous section. Information privacy goals can be achieved through privacy preserving mechanisms such as access control, privacy policies, and privacy preferences.

2.3.2 Walled Garden

In a toy computing environment, the concern is with the privacy of the user and that access to resources that can reveal context data are limited to the toy/game service

application, and only used for purposes which comply with privacy regulations and are acceptable to the user. While the toy computing environment follows a BYOD model, it is required to identify a privacy preserving BYOD architecture. The Whitehouse has outlined three high-level means of implementing a BYOD program [25]**:**

- **Virtualization**: Provide remote access to computing resources so that no data or corporate application processing is stored or conducted on the personal device;
- **Walled garden**: Contain data or corporate application processing within a secure application on the personal device so that it is segregated from personal data;
- **Limited separation**: Allow comingled corporate and personal data and/or application processing on the personal device with policies enacted to ensure minimum security controls are still satisfied.

In this context, a virtualized model would not be feasible or able achieve the privacy goals in a toy computing environment. However, privacy and security can be protected in a toy computing environment through the Walled Garden or Limited Separation approach. Walled Garden is a sandboxed and separated model which allows for processing to take place within a secure application which is separate from other applications and data. Limited separation allows the personal and corporate data and processing to comingle together, but enacts policies to protect the data and resources. Limited separation approach raises the issue of having a trusted mechanism for policy enforcement. To our best knowledge, not many research works are discussing the concept of Walled Garden.

2.3.3 Access Control

Access control is a security and privacy concept which aims to protect access to resources or data. The purpose of access control is to limit the actions or operations that a legitimate user can perform [88]. There are two parts related to access control: the access decision, and the access enforcement. Access decisions can vary but the most basic are permit or deny. Access control decisions are made based on policies, for a variety of purposes. There are several different approaches to access control, including

Mandatory Access Control (MAC) and Discretionary Access Control (DAC) [89], Role-based Access Control (RBAC) and Attribute-based Access Control (ABAC). In a DAC model, access decisions are based on the identity of users and/or membership in certain groups. Data owners are responsible for determining the type of access available to their resources. In MAC, sensitivity labels are assigned to users and resources. In this model, users are granted or denied access based on their security clearance and the label associated with the resource. Further, RBAC determines access to resources/data based on the role of the subject. Attribute-based access control makes access decisions based on attributes associated with subjects and objects. Access control

There are different types of policies which an access decision can be based on, e.g. privacy policies and security policies. Security policies are focused on maintaining confidentiality, integrity and availability of resources, while privacy policies are concerned with how and why data is used/shared/stored/etc. Privacy policies are the focus of access control decisions for the purpose of this work, and will be further described in the next section.

2.3.4 Privacy Policies and Preferences

Privacy policies describe an enterprise's data practices. This includes a description of what information is collected from users, what the information will be used for, how long it will be held, if/how the information will be shared to third parties, how long the information will be retained, etc. Consent is given by the user either implicitly or explicitly. Often, consent is implied just by using the services. Explicit consent can be given if the user is required to click "I agree" in regards to the privacy policy terms and conditions in order to receive services. Privacy policies are used for a company to outline their privacy practices relating to collection, use, retention, and sharing practices. Privacy preferences allow the user to create a set of rules to express how they wish their information to be managed.

2.3.4.1 Human Readable Policies

Privacy policies are often provided to their users in natural language. Mobile applications often provide privacy policies to their users in this format. The purpose of these privacy policies is to provide the user with the details on why and how their information is collected while they are using the mobile application. As an illustration, the following is the *Furby Boom!* App Privacy Policy, available online or through the app:

> Hasbro may collect non-personally identifiable information from devices that have installed a Hasbro app. This information is used to deliver services requested by users, such as content and updates within the app, as well as to support the internal operations of the app. For more information about the app, please contact us at http://hasbro-new.custhelp.com/ [90]

This policy is available before installing the application, and provides the user with an idea of what type of information is collected, and what the purpose is for its collection. This human-readable privacy policy is short and in simple terms, however it does not provide any detail on what information is actually collected, or how exactly it is used.

There are several concerns with how privacy policies are used in practice. In the case where a privacy policy is provided, the majority of users find them too complicated or long to read. Alternatively, as in the case of the *Furby Boom!* Privacy Policy, they can also be too vague. Human-readable privacy policies have a lot of limitations, some of which can be improved through the use of machine-readable policies.

2.3.4.2 XML and Machine Readable Policies

Structured policy languages allow for automated enforcement of privacy policies and access decisions. A privacy policy language supports access constraints (e.g. which subject can perform which action on which resource), as well as a description of access conditions. Policy languages must be platform independent, and able to integrate with the language used for access control policies [91]. Privacy policies can be expressed in eXtensible Markup Language (XML) [92] through policy assertion languages. XML is a flexible markup language used to describe data. XML is both human readable and

machine readable, and many APIs have been developed for processing XML data. Various languages and tools have been developed for the specification of privacy policies and preferences based on XML, including P3P, EPAL, XACML, and WS-policy.

Platform for Privacy Preferences (P3P)

Machine-readable privacy policy frameworks differ from human-readable ones. With machine-readable privacy policies, it allows the user to have more control over what information is collected and stored. Platform for Privacy Preferences (P3P) is a privacy policy framework created by the World Wide Web Consortium (W3C), based on XML designed to help end users manage their privacy while navigating websites that have differing privacy policies. User's privacy preferences are expressed using APPEL, A P3P Preference Exchange Language P3P also enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by users of P3P browsers [93]. P3P addresses user concerns about the type and number of data gathered by websites. At its most basic, any website that collects user information must clearly declare the reasons for the data collection, how it plans to use the information, and the amount of time it will retain the information. When using a P3P-compliant browser, cookies will be accepted, bypassed or denied depending on the previously mentioned user preferences. The user receives an alert when any privacy concerns arise and can override the previously set privacy level if they wish.

While P3P was primarily designed for Web sites, it has been the focus of many future directions including Web services and mobile services. In [94], adaptation for the mobile environment is noted as a prominent future direction for P3P. Some major research questions are also addressed in this paper, including: how to create mobile-based privacy user agents that can communicate compact privacy policies of mobile web sites or applications to users, and how to delegate automatic access control privileges to mobile applications and websites based on user defined privacy preferences. Some concerns with moving P3P to the mobile environment, as outlined in [95], include

performance, security of the policies, extending P3P vocabulary for the mobile environment, and adapting the user interface for use on small mobile devices.

The traditional approach to P3P has several shortfalls in terms of enforcement. [96] reiterates how P3P has not been strongly embraced in practice. Popular websites such as Google and Facebook have published P3P "compact policies" [97]. These policies state in human-readable code "this is not a P3P policy," while in practice, the system interprets it as a valid policy. In these situations, websites are able to technically comply with requirements but do not provide any actual privacy enforcement.

The authors of [21] performed an analysis on over 3000 P3P policies from 100,000 web sites to determine the relationship of privacy policies compared to legal requirements. The results of this study indicated that the surveyed website privacy policy statements had a widespread lack of adherence to legal mandates. Another report from the Canadian Internet Policy and Public Interest Clinic [98] found similar results in a survey of 72 Canadian websites showing widespread noncompliance with PIPEDA. Many businesses are not taking necessary steps to preserve the privacy of their users. Another issue is faced by international web service companies (e.g. Google and Yahoo), who have difficulty with privacy regulation while they are required to address a multitude of different or conflicting international privacy laws and jurisdictions that must be negotiated [21].

Enterprise Privacy Authorization Language (EPAL)

EPAL [99] is another XML-based privacy policy language by W3C member IBM, designed to formalize internal privacy practices of an enterprise. EPAL is more suitable than P3P to express internal privacy policies that can be enforced by the enterprise's privacy management system. EPAL allows an enterprise to define its own list of data categories, data users, purposes, and actions, whereas P3P is limited to a predefined list [100].

eXtensible Access Control Markup Language (XACML)

eXtensible Access Control Markup Language (XACML) [11] is an OASIS standard for access control language and architecture. The policy language uses the XML standard to define the policy and access control decision request and response. When there is an access request, an authorization decision/response can then be made based on the policy. XACML supports both centralized and decentralized policy management. XACML architecture uses the IETF Abstract Model for Policy Enforcement, which is further described in Section 2.3.5.

XACML specifies an abstract format for the authorization decision request as a description of the attempted resource access in terms of attributes [91]. An XACML attribute is associated with one of four classes: Subject, Resource, Action, and Environment. Subject is the entity who is sending the access request, Resource is the resource that is to be accessed, and Action is the action to be performed on the resource (e.g. read or write). The environment attribute describes an additional characteristic of the request such as time of day.

The use of XACML has been widely adopted in Web services [91]. A comparison between EPAL and XACML by Anderson [91], has recommended XACML for its functionality and flexibility. Lastly, Geospatial eXtensible Access Control Markup Language (GeoXACML) [101] is an extension to XACML Version 2.0. by the Open Geospatial Consortium designed to control access to geospatial information. GeoXACML supports four types of functions: topological, geometric, bag & set, and conversion to manage geospacial information.

2.3.5 Abstract Model for Policy Enforcement

A privacy policy alone does not guarantee that the policies will actually be enforced. This brings us onto the Abstract Model for Policy Enforcement proposed by IETF (terminology [102], model [103]) and ISO [104]. This model has been used for policy enforcement for privacy policy languages such as EPAL and XACML.

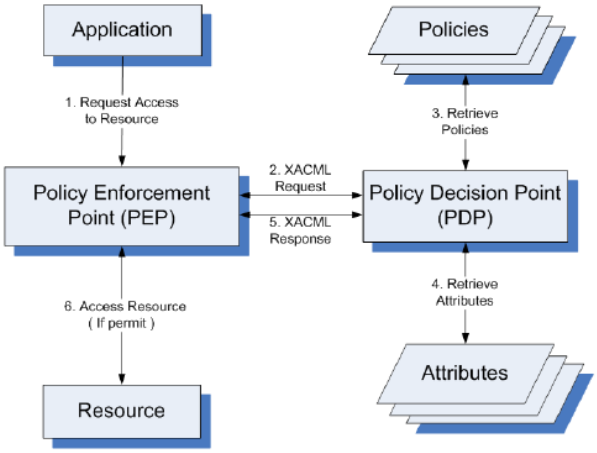

Figure 2.9 IETF Abstract Model for Policy Enforcement. Adapted from [105].

Referring to Figure 2.9, access control decisions are made by the Policy Decision Point (PDP), and enforced by the Policy Enforcement Point (PEP). When an application requests access to a resource, it sends the request to the PEP, which forwards the request to the PDP. The PDP then retrieves the policies and attributes to determine if the request complies. The PDP will make a decision and send a Permit or Deny response back to the PEP. The PEP will enforce the decision accordingly, providing access to the resource if permitted.

2.4 Related Works

There exist a number of previous works in the fields of privacy, mobile services, and location-based services. To the best of our knowledge, no previous work exists which identifies a framework for privacy exclusively in the context of toy computing, and especially with a focus on location. Further, although there has been work on the topic, there exists no widely accepted framework for privacy for any type of mobile services. This section will provide the reader with an overview of existing literature related to these topics.

2.4.1 Mobile and Web Services Privacy Frameworks

Hung et al. [74] describe a vocabulary-independent privacy authorization language framework for Web services which addresses the privacy requirements (AC020) defined by the World Wide Web Consortium (W3C) in their Web Services Architecture (WSA)

Requirements [106]. The framework recommends domain-specific vocabularies to be developed for different types of business applications (e.g. finance, healthcare, etc.). The authors introduce a protocol for enforcing privacy policies, in which privacy policies are described in P3P, and preferences exchange rules in APPEL. The paper also considers the use of privacy authorization language in other Web services-related languages such as WS-Policy, WS-Security, and WS-Privacy.

Access control is another area in which privacy is becoming more important. Traditional access control mechanisms such as discretionary access control (DAC), mandatory access control (MAC), and role based access control (RBAC) are not generally designed to accommodate privacy [107], however some recent RBAC extensions have been introduced with a privacy-focused objective [108]. Context- and location-based access control models have also been proposed [109], where certain services and data can only be accessed in a certain context/location. This is especially useful in a BYOD scenario where users wish to separate work from personal activities depending on their context.

A lattice-based privacy aware access control (LPAAC) model is described in [110], in which data provider and collector privacy preferences are accommodated and enforced. This model allows the data collector to identify their privacy policies for purpose, visibility, granularity, and retention of data in terms of minimal acceptance limit (MinAL) and maximal acceptance limit (MaxAL). The data provider can then review the privacy policies and select their own preferences within the range, allowing them to receive services from the data collector while still being in control of their data. This paper also identifies the importance of enforcement, and provides an algorithm based on the above for determining the access decision to be enforced by the system it is being implemented on. The authors have also implemented their model using P3P [111].

ipShield, introduced by [57], is a privacy-aware framework designed to quantify an adversary's knowledge regarding the user's context and obscure it before sharing. This framework does not depend on the user being anonymous, but instead focuses on choosing which data to share. It identifies several information disclosure systems, each

corresponding to a specific privacy-utility tradeoff. Also introduces privacy mechanisms designed to realize those tradeoff points. Chakraborty et al. [112] propose a framework for protecting data against unwanted inferences. This technique involves a white list of inferences that are desirable and provide utility, as well as a black list for unwanted inferences that should be kept private. From there, the authors attempt to define how much the recipient can infer from shared data based on utility-privacy parameters. They identify bounds on the parameters and provide mechanisms for achieving the bounds.

2.4.2 Location Privacy Techniques

Various techniques have been used in attempt to preserve the privacy of a user's location. Different approaches could involve or not involve a trusted third party [113]. Some approaches include degrading the quality of location information (obfuscation) [114] [115], creating fake location points [116], uncertainty [117] [118], pseudonyms [119], encryption [120] [121], and k-anonymity [122]. Policy-based access control is another technique which is used to decide whether a requesting subject can perform a given action on a data object. Various approaches for context-aware access control have been explored, which can also be used to preserve location privacy [123].

IETF RFC6280 by Barnes et al. [124] presents Geopriv, an architecture for location and location privacy in Internet applications. Geopriv is an Internet Best Current Practice, which enables users to express preferences for the disclosure of their location information. For example, the user can make a rule that their location is not to be disclosed beyond the intended recipient. This architecture binds the privacy rules to the data so that receiving entities are informed of when their data is shared to other parties.

2.5 Chapter Summary

In this chapter, we provided a background on the concept of toy computing, including the concepts of mobile services and physical computing. Next, we established a foundation on privacy in this context, including a description of XML-based privacy policy assertion languages including P3P and XACML. Finally, we provided an overview of some related works on mobile/web services privacy frameworks and location privacy.

Chapter 3 Privacy Requirements in Toy Computing

This chapter outlines the privacy requirements for a toy computing environment. The unique architecture of toy computing requires consideration of several different factors. In this chapter we investigate the privacy requirements through formal threat modeling techniques to help the reader to get more comfortable with the toy computing architecture and how it maps to privacy threats. Next, we identify privacy requirements at legislative level, identifying privacy laws and regulations which apply to this context. The toy industry has also issued regulations for toy safety; however these regulations have no mention of privacy. While parents aim to protect the privacy of their children, we investigate the unique requirements of end users.

3.1 Privacy Issues in Toy Computing

Table 3.1 outlines a comparison between a traditional toy, electronic toy, and toy computing. This illustrates how toy computing has evolved into a new paradigm, which inspires unique privacy concerns for children. Traditionally, toys have been entirely autonomous and do not have any processing capabilities or communicate with any other device. While a child user is engaged with a traditional toy, it will collect and store no personal data, and require no reason for concern for a child's privacy.

With the introduction of electronic toys with embedded systems, electronic toys can have sensory capabilities, and the ability to collect and store inputted data based on the user's interactions. This data is limited and used only for the interaction, often discarded immediately. While an electronic toy has the potential to collect and store user data, it operates on an entirely autonomous platform as a Trusted Computing Base (TCB). An electronic toy has limited or no networking capability. Thus, privacy concerns are limited to nonexistent in this architecture.

As outlined in Chapter 2, toy computing inherits the privacy concerns associated with mobile devices and BYOD. While toy computing technology allocates computing power to a mobile device, this is outside of the TCB and the device is untrusted. A mobile device also has the capability to collect a wide range of context information on the user, including their location data. Toy computing architecture allows and often requires information to be shared to services and other users. One of the most prominent concerns to privacy for toy computing compared to traditional and electronic toys is the networking capability which allows for the possibility of sharing information over a network. A mobile service is able to connect through a network to many other entities, including other mobile and Web services, servers, devices, and other users. While the mobile service has this ability to connect to and communicate with an extensive and possibly unknown amount of external entities, the issue of data sharing becomes a concern.

Table 3.1 Comparison of Traditional Toys, Electronic Toys, and Toy Computing

	Traditional Toy	**Electronic Toy**	**Toy Computing**
Interaction Medium	• Physical • Mechanical	• Physical (buttons) • Sensors – e.g. light, motion	• Physical – touch • Visual – camera • Auditory – microphone • Sensors – GPS, motion sensors, etc. • Wireless interface (network)
Data Collection	None	Limited	High - pervasive
Data Sharing	N/A	Limited or none	Many recipients
Potential to Collect Location data	No	Maybe	Yes
Processing Capabilities	N/A	Yes - limited	Yes - advanced
Networking	N/A	Limited or none	• Communicates with

Capabilities			other devices and services • Wi-Fi, Bluetooth, NFC, RFID, USB
Data Storage	N/A	Limited to device	• On Device (flash memory, SD card) • External to device (cloud, database, server)
Architecture and TCB	Autonomous Trusted	Autonomous Trusted	BYOD – device is untrusted
Platform	Closed	Closed	Open

These threats can be summarized as the following three items that affect the privacy in toy computing.

1. Child's Identity
2. Location Data
3. Networking Capabilities

When a child engages in toy computing activities, their identity is associated with the data collected from the device. The mobile service connects to other entities over a network and shares the data. This reveals the unique privacy issues of toy computing: when a child engages with a toy computing toy, the child's identity is associated with their location data and can be shared over a network. This unique threat architecture is illustrated in Figure 3.1.

This sharing of sensitive location data opens up vulnerabilities such as customer profiling of minors, and child predators. Customer profiling of minors involves accessing collected data to create portfolios of users related to their location history (e.g. the ability to collect data on when and where a user was, including travel patterns). This is typically used for online marketing, however location data allows for tracking and inferences on user behavior that is not otherwise publically available. Further, when

physical location data is being shared with other users, it is important to consider a child's physical safety in regards to child predators who could potentially locate them based on learning their GPS location, possibly paired with other sensitive data.

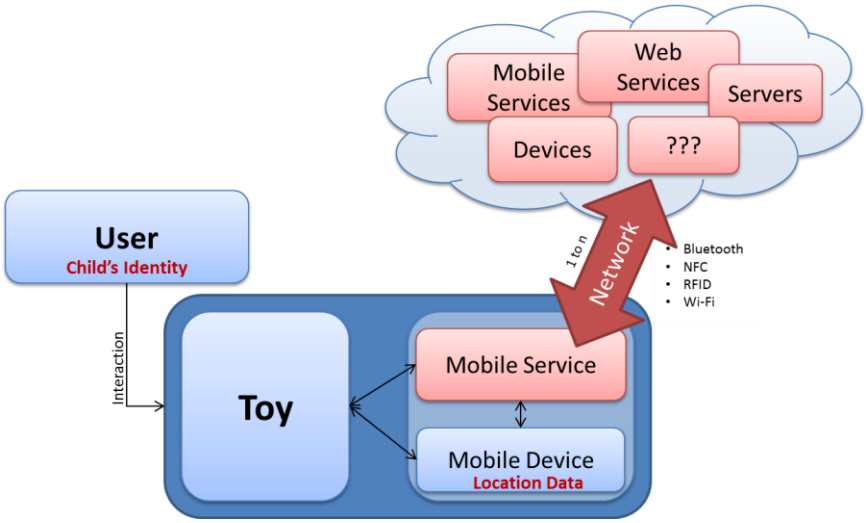

Figure 3.1 Child Identity and External Parties

While these privacy issues are common in the domains of mobile and online privacy, they are relatively new to the domain of toys. Due to the mainly child user base, and the physical toy component, toy computing separates itself from the other categories and identifies as a unique area for privacy concerns. Table 3.2 provides a comparison between the three categories of toys, as well as online/mobile services, illustrating the unique privacy concerns of toy computing.

Table 3.2 Privacy Concerns in Toy Computing

	Traditional Toy	**Electronic Toy**	**Toy Computing**	**Online/Mobile Services/Applications**
Physical Toy	X	X	X	
Child's Identity	X	X	X	X
Collects Data		X	X	X
Networking Capability		Maybe	X	X
BYOD model			X	X

Toy computing technology which embraces sensory and networking capabilities opens up new threats to privacy, stimulates new user requirements, and establishes a unique case for existing laws and regulations. Toy computing inherits laws and regulations from the components that make it up (services, mobile, toys), however, there are no laws that explicitly regulate the unique environment of toy computing. There is also no widely adopted framework to allow parents to manage the privacy of their children using toy computing technology. For this reason it is necessary to outline the privacy requirements to present a solution to managing location privacy for a toy computing environment.

3.2 Privacy Threat Model

In this section, we investigate the privacy of toy computing from a threat modeling perspective. Threat modeling is a useful tool to assess risk associated with a system and provides a structured approach to security and privacy. Threat modeling can be included as part of the Software Development Lifecycle (SDL). In this section, we aim to identify location privacy threats in a toy computing environment. We present a privacy threat model for toy computing with a focus on location privacy.

3.2.1 Threat Modeling Techniques

Several approaches have been developed for threat modeling, one of the most widely adapted being Microsoft's Threat Modeling Process [125] (illustrated in Figure 3.2) and STRIDE Model [126] for identifying six categories of security threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. This model presents an excellent approach to understanding and decomposing an application to identify security threats, however there is little focus on privacy. In order to preserve privacy, there must be a foundation of security. To achieve this, it must be ensured that the system has a reasonable level of security mechanisms in place, and that personal information is protected from a security perspective. While the focus

of this thesis is on privacy, we will assume that the system has a reasonable level of security.

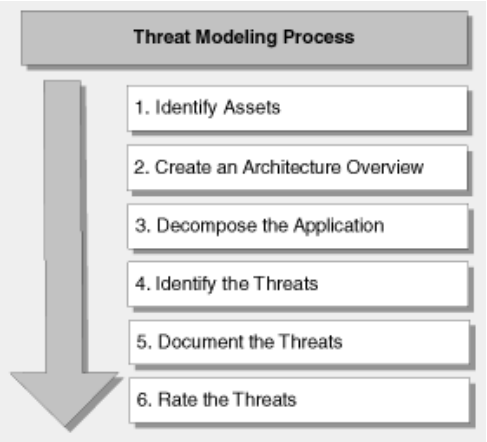

Figure 3.2 Microsoft's Threat Modeling Process. Adapted from [94]

The Open Web Application Security Project (OWASP) has developed their own Application Threat Model [127] which has some similarities to Microsoft's model. Based on this model, OWASP has also developed a Mobile Threat Model [128] to identify security threats specifically for mobile applications. OWASP also recommends Microsoft's STRIDE model for identifying threats. We found this useful to consider in a threat model for toy computing, which occurs in a mobile environment. However, this model once again has little focus on privacy.

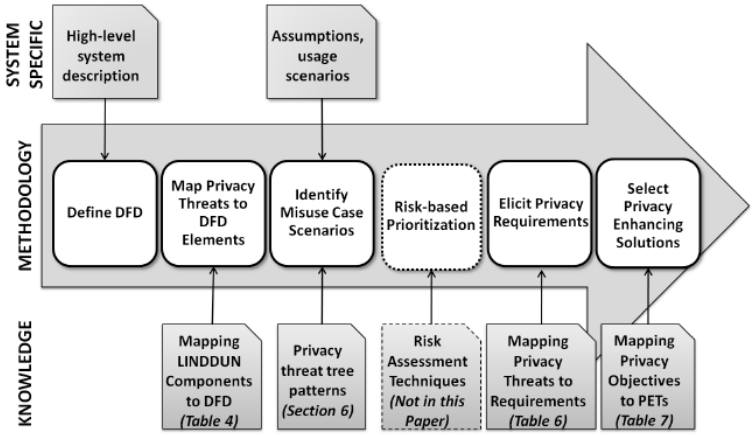

Figure 3.3 LINDDUN Threat Modeling Process, adapted from [99]

While both of the above models are primarily concerned with security, there is no widely adopted framework for modeling privacy threats, especially in mobile environments [129]. Deng et al. [130] [131] have developed a methodology called LINDDUN which provides a comprehensive privacy threat modeling framework. Figure 3.3 illustrates the threat modeling steps in the LINDDUN methodology.

Like the STRIDE and OWASP models, LINDDUN identifies privacy threats by data flow elements and maps them to privacy threats. Misuse case scenarios and privacy threat tree patterns illustrate privacy attack scenarios, which are then prioritized through risk assessment techniques. In the final two steps of this method, mapping the privacy threats to privacy requirements allows for the identification of privacy enhancing solutions. The LINDDUN methodology provides an excellent framework for modeling privacy, although it was not designed for mobile applications in particular. LINDDUN was adapted from the STRIDE model [125], using similar threat modeling principles (data flow diagrams, threat trees and trust boundaries) and mapping them to privacy properties based on the terminology defined by Pfitzmann et al. [132]. These privacy threats described below are the basis of the LINDDUN methodology and widely recognized in the privacy research community:

1. **Linkability** – An attacker is able to distinguish whether two or more items of interest (e.g. subjects, messages, actions, etc.) are related or not within the system.
2. **Identifiability** – An attacker can sufficiently identify a subject associated to an item of interest, for example, the sender of a message. Usually, identifiability refers to a set of potential subjects. This is a special case of linkability between a subject and its attributes. Identifiability is a threat to anonymity and pseudonimity.
3. **Non-repudiation** – This allows an attacker to gather evidence to counter the claims of the repudiating party and to prove that a user knows, has done or has said something.
4. **Detectability** – An attacker can sufficiently distinguish whether an item exists or not (e.g. messages are sufficiently discernible from random noise).

5. **Information Disclosure** – Personal information is exposed to individuals who are not supposed to have access to it.
6. **Content unawareness**- A user is unaware of the information disclosed to the system. The user either provides too much information which allows an attacker to easily retrieve the user's identity or inaccurate information which can cause wrong decisions or actions.
7. **Policy and Consent Noncompliance** – This means that even though the system shows its privacy policies to its users, there is no guarantee that the system actually complies to the advertised policies. Therefore, the user's personal data might still be revealed.

The above threats can be categorized into hard or soft privacy threats [131]. Our focus for this thesis is on soft privacy: information disclosure and content awareness. Soft privacy is based on the assumption that the data subject is not in control of personal data, and must trust the data controllers (service providers). This is the domain of policies, access control and audit. In this model, the data subject provides personal data and the data controller is responsible for it. Policy consent and noncompliance is beyond the scope of this work, which assumes that the system complies with its privacy policies.

3.2.1.1 Our Approach

Based on the above threat modeling techniques, we have adapted our own technique appropriate for modeling privacy threats in a mobile toy computing environment. Below is the threat modeling process we will be covering in the following sections, adapted from Microsoft's Threat Modeling Principles [125] and STRIDE Model [126], OWASP's Mobile Threat Model [128], and the LINDDUN methodology for privacy threat analysis by Deng et al. [131]. We believe that this will provide an effective analysis of privacy threats in a mobile toy computing environment.

Our approach, illustrated in Figure 3.4, uses a similar process as the three models discussed, with greatest motivation from LINDDUN. Starting with an overview of the technical architecture, we will identify location data assets and data flow. Next we will

use the LINDDUN methodology to identify privacy threats and threat agents, and illustrate methods of attack through threat trees. Lastly we will use this analysis to identify privacy requirements and controls to mitigate threats to location privacy.

Figure 3.4 Threat Modeling Process

3.2.2 Architecture Overview

A toy computing application allows the user to interact with a physical toy device along with a mobile device to play a game. From an architectural perspective, we will consider the end user components (the user, physical toy component, and mobile device) as one entity, which in our diagram will be referred to simply as the *mobile device*. The user is the individual who is playing with the toy, which is connected to a mobile device also operated by the user. The user interacts with the physical toy and/or mobile device through touch screen, microphone, camera, and/or other sensors such as the accelerometer. The physical toy component may or may not have embedded systems, but must be able to interact in some way with the mobile device (ex. physically, visually, audibly, or through a wireless interface). The toy computing environment follows the BYOD model, where the mobile device is provided by the user and may take the form of a smartphone or tablet. GPS location data is also collected and stored on the mobile device. Data is stored on the device in flash memory and/or removable storage (i.e. SD card), and communicated over wireless interfaces such as Wi-Fi, Bluetooth, NFC, or RFID.

3.2.3 Assets and Data Flow

3.2.3.1 Identify Assets

With a focus on location privacy, potential sensitive data that could be collected on the user is as follows. Location data is collected through the GPS on the mobile device. As discussed in Chapter 2, location can be expressed as absolute, relative, or type of

location. For the purpose of this scenario, we are concerned with absolute location, which is the location expressed in a range or exact GPS coordinates, latitude and longitude. The absolute location can be expressed as coarse or fine [61]. The location can be collected as a single GPS location event (the location of the user at one point in time), or a GPS trace (a series of location events recorded over a period of time, showing location history). A GPS location includes a timestamp for the time it was detected. The location of the user may be directly or indirectly associated with their real identity and other profile data. In the case of toy computing, the user is a child under the age of 13, their personal information is particularly sensitive, especially when associated with their real identity. Alternatively, location data may be anonymous or associated with a pseudonym. This depends on the architecture and privacy practices of the specific application and service provider, and is beyond the scope of this thesis. Our focus is on enabling the user to be in control of their privacy by specifying their privacy preferences, under the assumption that the service has published an accurate privacy policy and also complies with it. Inferences can be made based on GPS location combined with other data such as:

- Type of motion (walking, standing, running, driving, etc.).
- Interactions with other users, friends in same location (e.g. who they are with at a certain time/day).
- User's real identity associated with their location (name, age, profile data).
- Behavior (e.g. religious beliefs based on going to church, or health based on frequent doctor's appointments).
- Location of home, school or daycare.
- Travel patterns (e.g. where they are likely to be at a given time or day).
- If a child is home and parents may not be (e.g. during work hours), or alternatively if a child is in a public place while a parent may not be.

From the service provider's perspective, it is necessary to collect this data for the purpose of running the game. Parents who wish to be in control of their child's private

location data may limit the collection of this data under certain contexts depending on a company's privacy policies.

3.2.3.2 Data Flow

Use Case Application - Blaster Toy First-Person-Shooter (FPS) Game

When a game starts, the mobile device connects to mobile service(s) which support gameplay. For the case of this study with a focus on location privacy, the mobile service receives GPS location data on the user and responds with location-based services such as the location of other players. Also connected to the service are other players, and other potential third parties. A blaster toy first-person-shooter (FPS) game, such as *Tek Recon* (discussed in Chapter 2), will be used as a use case application throughout this section. *Tek Recon* a multiplayer mobile toy computing environment, where users participate in a game with their friends through a mobile application over a network. With our focus on location privacy, the game uses GPS location data from all of the users' mobile devices so they can locate each other on the map.

In the DFD illustrated in Figure 3.5, the user is represented as a 3-tuple entity (user, toy, mobile device) which interacts with the system. The toy computing environment contains two processes: the mobile service and the walled garden module. While a user is engaged in the game, they interact with the physical toy and the mobile device, and the mobile device is connected to a mobile service, which may be connected to other entities over a network. GPS location data is collected from the user from the GPS on the device. When the mobile service sends a request for the location data, the mobile device forwards the request to the walled garden module, which checks the policies and makes an access control decision for the request. If the request is permitted, the mobile device then responds to the mobile service with the requested location data.

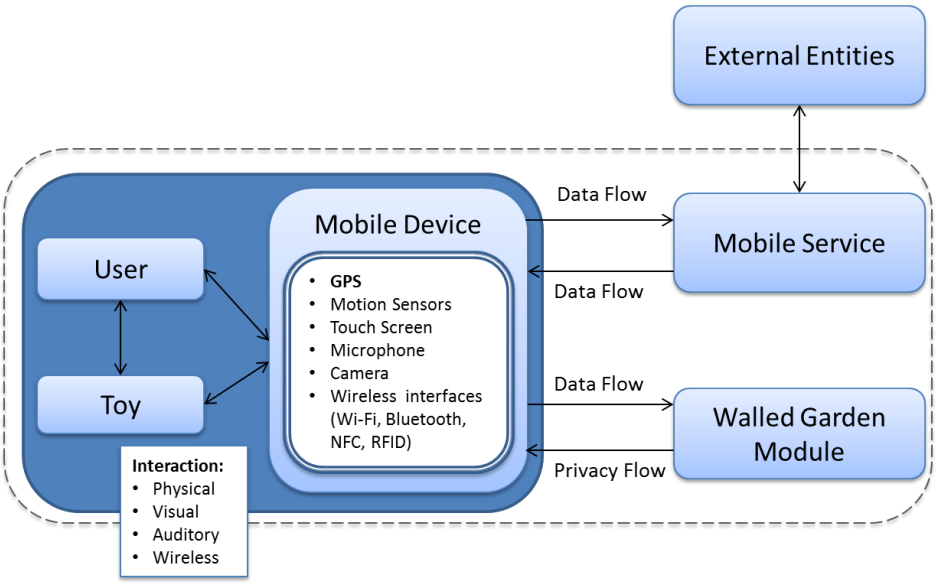

Figure 3.5 Tek Recon Game Data Flow Diagram

3.2.4 Privacy Threats

3.2.4.1 Identify Privacy Threats

From a policy perspective, any data sharing practices that may result in any of the above LINDDUN threats should be identified in the system's privacy policy. This work depends heavily on the assumption that the service has published an accurate privacy policy and also complies with it. For the purpose of this thesis, we aim to address the threats of information disclosure and content unawareness. Information disclosure occurs when a user's personal information is exposed to individuals who are not supposed to have access to it. For the purpose of this work we will assume that although the information disclosure practices are outlined in the privacy policy, and the user has provided their consent, the user is not actually aware due to the face that they did not read or understand the policy. Content Unawareness occurs when the user is unaware of the information that is collected on them, for example their location information. Looking at these threats in more detail, the IETF's RFC6973 on Privacy Considerations [133] provides more specific secondary threats which fall under the categories of Information Disclosure and Content Unawareness. In the model, we attempt to prevent all four of these categories of threats to children:

- **Surveillance**: "the observation or monitoring of an individual's communications or activities. The effects of surveillance on the individual can range from anxiety and discomfort to behavioral changes such as inhibition and self-censorship, and even to the perpetration of violence against the individual. The individual need not be aware of the surveillance for it to impact his or her privacy – the possibility of surveillance may be enough to harm individual autonomy."
- **Secondary Use**: the use of collected information about an individual without the individual's consent for a purpose different from that for which the information was collected. Secondary use may violate people's expectations or desires. The potential for secondary use can generate uncertainty as to how one's information will be used in the future, potentially discouraging information exchange in the first place.
- **Disclosure**: Disclosure is the revelation of information about an individual that affects the way others judge the individual. Disclosure can violate individuals' expectations of the confidentiality of the data they share. The threat of disclosure may deter people from engaging in certain activities for fear of reputational harm, or simply because they do not wish to be observed.
- **Exclusion:** Exclusion is the failure to allow individuals to know about the data that others have about them and to participate in its handling and use. Exclusion reduces accountability on the part of entities that maintain information about people and creates a sense of vulnerability in relation to individuals' ability to control how information about them is collected and used.

3.2.4.2 Mapping Privacy Threats to DFD

Referencing the DFD from Figure 3.5, we will now outline the DFD elements and then map the privacy threats to the DFD. Table 3.3 shows the DFD elements in the Blaster FPS Game mentioned in the previous section.

Table 3.3 Mapping Blaster FPS Game DFD Elements to Privacy Threats

Entity	User
Process	Game

	Service
Data Store	User's Location Resources on Mobile Device Service Database (DB)
Data Flow	User data stream (user to game) Service data stream (game to service) DB data stream (service to DB)

Now based on the above DFD elements, in Table 3.4 we map the LINDDUN privacy threats to DFD element types (E: Entity, DF: data flow, DS: data store, P: process) in a toy computing scenario with the Tek Recon example:

Table 3.4 Mapping Privacy Threats to DFD Elements

Threat Categories	**Entity**	**Process**	**Data Store**	**Data Flow**
Linkability	x	x	x	x
Identifiability	x	x	x	x
Non-repudiation		x	x	x
Detectability		x	x	x
Information **D**isclosure	T	A	A	A
Content **U**nawareness	T			
Policy/Consent **N**oncompliance		A	A	A

Legend: [x = Out of Scope, T = Threats addressed, A = Assumed to Comply]

The threat of information disclosure occurs at the process, data store, and data flow levels. This falls into the control of the service provider, who outlines information disclosure practices in their privacy policy. While we assume that the service has accurate policies and also complies with them, the threat we are concerned with is then with the entity who agrees to disclose the information. Content unawareness is a threat to the entity (user). The user is required to provide the necessary consent to process personal data. The goal of our model is to address the threats of Content Unawareness from the perspective of the user, putting them in control of information disclosure. This

model will address information disclosure from the entity (user)'s perspective who complies with information disclosure practices. This model is acting under the assumption that the process, data store, and data flow elements all act in compliance with their policies and the consent of the user.

3.2.5 Methods of Attack

In this section we will observe different methods an attacker can use to reach the data. First we will examine privacy threats based on Table 3.3 in the previous section to determine privacy threat trees. Next, we will create misuse case scenarios based on the threat tree patterns.

3.2.5.1 Privacy Threat Trees

Information Disclosure

Figure 3.6 refers to the privacy threat tree for information disclosure. For the purpose of this work, we are referring to intentional information disclosure, which is predefined by the service and outlined in the privacy policy, rather than information disclosure as a result of security exploits. Information disclosure can occur at process, data store, or data flow level. Location information may be disclosed to other users or with a third party. The threats related to sharing an entity's location data can lead to undesirable inferences of the user's behavior and personal life (see list of inferences in Section 3.2.3). A child's location data sent to a third party can be used for customer profiling of the child. Sharing location data with other users puts the physical safety of the child user at risk if it is shared with an untrusted entity. For these reasons, a user may choose not to consent to sharing their location data depending on privacy policy practices.

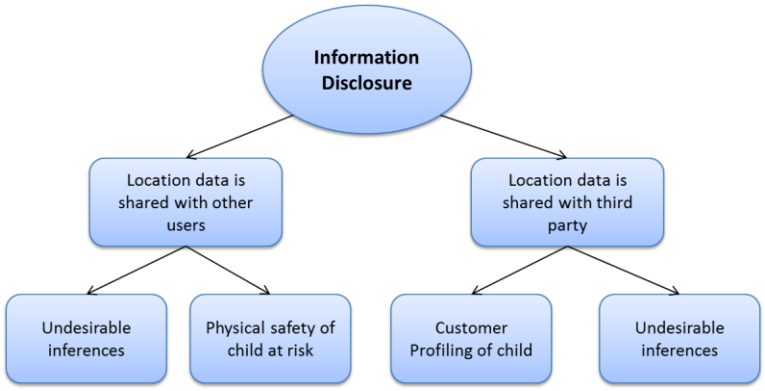

Figure 3.6 Information Disclosure Privacy Threat Tree

Content Unawareness of Entity

Content unawareness occurs at the user level when the user provides more personal data than is required, or does not read the privacy policies. Providing too much personal data is unnecessary and opens up opportunity for further undesirable inferences. It is also possible that a user does not read the privacy policies and therefore is unaware that certain aspects of their personal data is being collected and shared. The user may be unaware of the purpose their location data is collected, or how it is used. The user may not even be aware that their location information is being collected at all. Additionally, the user may not be aware that their location data is being shared with third parties. All of these situations can result in information disclosure (see previous section) to which the user has unknowingly provided their consent.

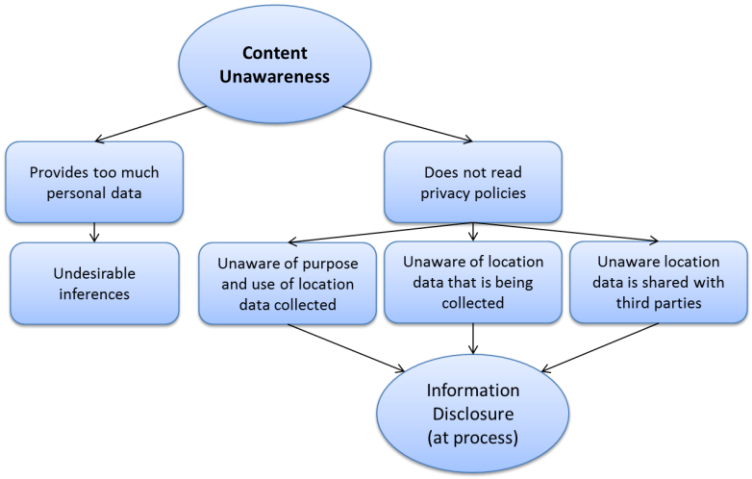

Figure 3.7 Content Unawareness Privacy Threat Tree

3.2.5.2 Misuse Case Scenarios

In this section we provide a misuse case scenario of Tek Recon based on the threat tree patterns in the previous section. The misuse case model is based on the LINDDUN model.

Content Unawareness and Information Disclosure

The threat trees in the previous section indicates that in order to be susceptible to the threat of content awareness, the user either unknowingly provides too much personal data, or does not read privacy policies. For information disclosure, the mobile service forwards the data to a third party or another user. These are the preconditions of the misuse case. To create the attack scenarios, the attacker first needs to have access to the data store, and either the user (data subject) can be re-identified or the pseudonyms can be linkable. In this scenario, the actions of the misactor are actually completely legitimate as outlined in their privacy policy, however the data use/sharing practices do not comply with the user's expectations or legislation.

Title: Misuse Case 1: Content Unawareness and Information Disclosure

Summary: User unknowingly provides location data to the service

Assets, stakeholders and threats: location information of the user. The parent/guardian and user are unaware the information is collected and sent. Potential threats: surveillance, secondary use, disclosure, exclusion

Primary Misactor: Parent/guardian for not reading privacy policy.

Basic Flow:

1. Parent/guardian consents to privacy policy without reading it.
2. User unknowingly sends location information to the mobile service.

Alternative Flow:

3. Same as the above, and the mobile service sends user's location information to a third party for marketing purposes.

Trigger: Parent/guardian does not read the privacy policy which outlines the mobile service's privacy practices.

Preconditions:

1. Parent/guardian provides consent but has not read or understood the privacy policies.
2. Parent/guardian and user have some sort of expectation for privacy which is does not actually correlate with the privacy policy or the data use/sharing practices of the service.

3.2.6 Privacy Requirements/Controls

Based on the above analysis of threats and attack scenarios, we now propose some privacy requirements and controls needed to mitigate these threats. The IETF outlines in their privacy considerations [133], two major mitigation techniques to deter threats of surveillance, disclosure, secondary use and exclusion. Techniques are data minimization and user participation:

- **Data Minimization:** limiting collection, use, disclosure, retention, identifiability, sensitivity, and access to personal data to the minimal amount necessary to perform a task. Reducing the amount of data exchanged reduces the amount of data that can be misused or leaked. Data Minimization mitigates the threats of: surveillance, secondary use, and disclosure.
- **User Participation**: data collection and use that happens "in secret," without the individual's knowledge, is apt to violate the individual's expectation of privacy and may create incentives for misuse of data. As a result, privacy regimes tend to include provisions to support informing individuals about data collection and use and involving them in decisions about the treatment of their data. In an engineering context, supporting the goal of user participation usually means providing ways for users to control the data that is shared about them. It may also mean providing ways for users to signal how they expect their data to be used and shared. User participation mitigates the threats of: surveillance, secondary use, disclosure, and exclusion.

Our threat model illustrates that the privacy requirements for toy computing are data minimization and user participation, in order to mitigate the threats of information disclosure and content unawareness, which can lead to surveillance, disclosure, secondary use and exclusion. Privacy controls which achieve the goals of data minimization and user participation include implementing a privacy access control model.

3.3 Privacy Considerations

3.3.1 End User Requirements for Children

Children provide a unique user base which requires special attention in several key areas related to their privacy. Firstly, it is widely accepted internationally that that a child's data is considered particularly sensitive and should be treated with extreme care [12] [13]. Online privacy for children has been a great concern, and this concern is inherited into the toy computing environment, particularly when the child's location is involved and can be potentially shared with other parties. Children must be protected from violence, sexual abuse and exploitation which they can be vulnerable to online including harassment, stalking, grooming, sexual abuse or exploitation, or personal data misuse [14]. Sexual solicitation and internet-initiated offline encounters are a major issue for the online safety of children [15]. The U.S. Department of Justice [16] indicates that "1 in 25 youths received an online sexual solicitation in which the solicitor tried to make offline contact." All of these risks are increased with the possibility of a potential solicitor becoming aware of the child's location or historical location patterns. On the other hand, children also take up a large segment of the consumer population and are of particular interest to market researchers who may attempt to collect their personal data and usage patterns for targeted advertising [17]. Third party advertisers can infer a great amount of information about a child based on their location and other context information, collecting detailed behavioral profiles that may be used for unknown or unwanted purposes.

Another concern with child users is that the usage patterns of children differ from that of an adult. Children often have little understanding or regard for the privacy of their information, and are more likely to act in spontaneous ways. The usage behavior of children indicates that they are more open to giving out personal information, which makes issues of sensitive data sharing of great concern. Child users exhibit a varying level of awareness when it comes to their online activities and understanding of privacy risks. There is a fluctuating level of comfort and knowledge with technology and online activities among children, where usage and online behavior differ according to their age, development level, and frequency of use. Children may lack the maturity to appreciate the wider social and personal consequences of revealing or agreeing to share their personal information online, or the use of their personal information for commercial purposes [13]. Younger children in particular generally lack the skills and confidence in areas of internet use that are especially important for safety [14]. In order to be effective, privacy protection strategies are required which incorporate measures and messages appropriate to different ages and levels of understanding [134].

The online mobile environment and associated toy computing technology provides many opportunities for children, but is also accompanied by several risks. Many initiatives have been undertaken in attempt to provide an online environment which is safe and age-appropriate, and to help children to be empowered and engaged in the online environment [135]. Organizations such as UNICEF have been working to promote digital citizenship among children and develop products and platforms that facilitate children's positive use of technology [13]. Noted by Westin [136], "each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire of disclosure and communication of himself to others." Several works such as [137] iterate the competing goals of utility vs. privacy. A popular theme in industry guidelines indicates a need for balance between children's right to protection from violence, sexual abuse and exploitation, and the right to information access, freedom of expression, privacy and non-discrimination [134]. Measures for protection must also not be overly restrictive for the child or other users [13]. It is

possible for some measures to challenge current business models, reduce the competitiveness of a company, or threaten other freedoms currently observed online [134]. The Toy Industry Association (TIA) has raised concerns that restrictions could limit the ability for toy companies to obtain necessary data to analyze and improve content, allow children to enjoy personalized but anonymous online experiences, and benefit from the ability to offer targeted advertising on their e-commerce and adult sites [138]. Thus it is necessary to find the appropriate balance between privacy and freedoms to users.

3.3.2 Parental Control

A report from Pew Research Center and Berkman Center for Internet & Society at Harvard University [139] indicates that the majority of parents in the United States are concerned about their children's online privacy, some of the main concerns being related to strangers online, and the data advertisers are collecting about their children's online behavior. While parents strive to ensure their child's physical and online safety and privacy, they may wish to be in control of how their personal data is shared through the devices they are using. The main protection children have on the Internet is parental guidance and supervision [17]. Privacy controls can allow parents to create policies to prevent their children from allowing their data to be collected from services according to their preferences. The ITU and UNICEF recommend parental controls "not to transfer responsibility for children's ICT use to parents alone, but to recognize that parents are in a better position to decide what is appropriate for their children and should be aware of all risks in order to better protect their children and empower them to take action" [13]**.** Parental controls can be rated by their functionality, effectiveness, usability, and security [140]:

- Functionality: Does the tool have the required functions for the parent's needs?
- Effectiveness: Does the tool successfully block the intended content or action?
- Usability: Is the tool easy to install, configure and use?
- Security: Does the tool prevent the child from bypassing or disabling the controls?

In regards to usability, parents sometimes have less understanding and knowledge of the internet and mobile devices than their children. Further, convergence of mobile devices and internet services makes parental oversight more difficult [13]. This introduces difficulties with a parent's ability to effectively implement privacy controls for their child. In a mobile toy computing environment, the child will likely be using either a mobile device belonging to his/her parent or using his/her own mobile device. Parents may face privacy challenges related to reviewing privacy policies of applications that they or their children may be using. A study by Chin et al. [141] of 60 participants found that users are highly likely to install free applications, and place a higher value on other user reviews than of privacy policies and EULAs.

Also, users often have more dangerous tendencies on their mobile behavior than they do on a computer or laptop. When reviewing privacy policies, parents are likely to face difficulty in reading and understanding the policies. A further study by Felt *et al.* [142] found that only 17% of participants paid attention to permissions during installation, and only 3% could correctly answer permission comprehension questions. It can be inferred from this research that the majority of users do not understand or care about the permission warnings that they receive on their mobile devices. This is a huge disadvantage to the current permissions system, illustrates the need to improve the usability of privacy protecting systems.

Peng et al. [143] discuss the importance of communicating the privacy risks of an application to users, while also proposing a method for ranking risks based on probabilistic generative models. It is understandable that parents will run into similar issues with understanding privacy practices in regards to their children. While they will also likely be even more concerned with their child's privacy, it is important to parents/guardians that they are able to understand and correctly control their child's private data. A privacy preserving framework is required to allow parents to easily and effectively set preferences to control and restrict the personal data that can be collected on their child.

3.3.3 Privacy Laws and Regulations

Privacy protection laws define the rights of data subjects (users), the responsibilities of data collectors (service providers), and methods for dispute resolution. These laws are generally enforced through ombudsmen (e.g. Privacy Commissioner of Canada), or licensing bureaus (e.g. CNIL in France) [21]. Different countries and legislations have different laws for privacy protection, and there are also many international guidelines and industry regulations which outline privacy best practices. These laws and regulations can also differ depending on what type of information is being collected (e.g. health information), or who the users are (e.g. children under the age of 13). In this thesis, we aim to investigate the privacy aspects relevant to the child users, toys and safety, and location data.

Toy computing encompasses a range of technologies, including traditional and electronic toys, internet, mobile devices, and inherits the privacy requirements and governing laws and regulations of each, with particular attention to children. Traditional distinctions between different parts of the telecommunications and mobile phone industries, and between internet companies and broadcasters, are fast breaking down or becoming irrelevant [13]. With the change in technology, regulating bodies have recently been striving to update laws, regulations and industry guidelines. Table 3.5 shows the privacy concerns associated with each technology and the corresponding laws and regulating organizations to address them.

Table 3.5 Privacy Concerns and Regulation Across Toy Computing Components

Component	**Traditional & Electronic Toys**	**Internet/Web Services**	**Mobile Apps/Services**
Children's Privacy Concerns	• physical safety	• Inappropriate content, conduct, or contact	• Pervasiveness • Location • BYOD
Laws and Regulation	• Toy Safety Guidelines • Toy Industry Association (TIA)	• PIPEDA (Canada) • COPPA (USA) • UNICEF/ITU Industry Guidelines	• MMA • CTIA

3.3.3.1 Privacy Principles

Canada's privacy laws are outlined in The Personal Information Protection and Electronic Documentation Act (PIPEDA) [19], which governs how personal information can be collected, used, and disclosed in commercial business. PIPEDA is based on the 10 principles of privacy outlined in the Canadian Standards Association's (CSA) Model Code for the Protection of Personal Information [144], which has been recognized as a national standard as of 1996 [22]. This model code is representative of principles behind privacy legislation in many countries, including the United States and the European Union. It also bears similarities to the Organization for Economic Cooperation and Development (OECD) Guidelines for the Protection of Privacy and Transborder Flows of Personal Data [145] which have been adopted by member countries of the European Union [146]. The CSA's 10 Principles of Privacy are summarized as follows [22]:

1. **Accountability** – an organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
2. **Identifying Purposes** – the purpose for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. **Consent** – The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except when appropriate.
4. **Limiting Collection** – the collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure, and Retention** – personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfillment of those purposes.
6. **Accuracy** – personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards** – personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. **Openness** – an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. **Individual Access** – upon request, an individual shall be informed of the existence, use and disclosure of his/her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging Compliance** – an individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

Children's Privacy Laws

PIPEDA does not mention any special regulations for children. While PIPEDA requires meaningful consent for the collection of personal data collection, it does not refer to a particular age threshold for this. There is a difficulty in determining if a child is able to provide meaningful consent, as this greatly depends on their cognitive and emotional development and their understanding of privacy and online practices [12]. The Office of the Privacy Commissioner of Canada (OPC) has indicated in the Online Behavioural Advertising Guidelines [24], a focus towards protecting children's online privacy particularly in the region of online behavioural targeted advertisements. The OPC recommends for organizations to avoid knowingly tracking children and websites aimed at children. The OPC has also made the following recommendations regarding the management of the personal information of children and youth [12], however these recommendations are not legally binding:

- Children's information is considered sensitive and merits special consideration under privacy laws.

- Organizations should implement innovative ways of presenting privacy information to children and youth that take into account their cognitive and emotional development and life experience.

The United States Federal Trade Commission (FTC) Children's Online Privacy Protection Act (COPPA) [23] protects the online privacy of children under the age of 13, and indicates that a child's personal information cannot be collected without parental consent. In 2010, an amendment to COPPA further elaborated that personal information includes geolocation information, photographs, and videos.

In the European Union, privacy laws are governed by the European Union Data Protection Directive (EUDPD) 95/46/EC [146], which also has special considerations for children under the age of 13. The Directive states that consent must be given by the child's parent or custodian, and must also be verifiable (Article 8). Further, the United Nations Convention on the Rights of the Child (CRC) [18] is the most widely endorsed international human rights treaty. This treaty protects children from all forms of violence, exploitation and abuse and discrimination, and ensures that the child's best interest should be the primary consideration in any matters affecting them. UNICEF defines children as individuals under the age of 18, according to Article 1 of the Convention on the Rights of a Child [13]**.**

Canada does not have an equivalent to COPPA, or any specific mention of children within PIPEDA. For the purpose of this work we will consider the recommendations by the OPC to preserve children's privacy. We will follow the direction of COPPA and the EUDPD in the definition of a child as an individual under the age of 13 years old. With this in mind, we aim to assist the parent/guardian in protecting the privacy of their child by putting them in control of the information of their child that is shared.

Location Privacy Laws

There do not appear to be special laws in place for regulating the privacy aspects of location data, however it is categorized as personal information is therefore covered by

PIPEDA. PIPEDA recognizes personal information in Section 2(1) as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." PIPEDA defines a *"record"* as including "any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things." An *"electronic document"* is defined by PIPEDA is "data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data." GPS data is not explicitly mentioned in either of these definitions, however it is possible that it could be considered included. In a 2006 PIPEDA case summary, tracking information collected from a GPS placed in company vehicles was acknowledged as personal information, "since the information can be linked to specific employees driving the vehicles. The employees are identifiable even if they are not identified at all times to all users of the system" (PIPEDA Case Summary #2006-351). In 2010, an amendment to COPPA further elaborated that personal information includes geolocation information, photographs, and videos. For the purpose of this work, we will consider COPPA's reference to geolocation information as a type of personal information to be protected.

Health Canada's Safety Requirements for Children's Toys and Related Products

In Canada, the Canada Consumer Product Safety Act (CCPSA) applies to all manufactures, importers, advertisers, sellers, or testers of a consumer product. A toy is defined by the Government of Canada's Toy Regulations [147] as "a product that is intended for use by a child in learning or play." Health Canada identifies a toy as intended for use by children less than 14 years of age, unless a younger age is prescribed within a requirement. This is consistent with several international toy safety standards [20]:

- ISO 8124-1 Safety of toys - Part 1: Safety aspects related to mechanical and physical properties
- EN71-1 Safety of toys - Part 1: Mechanical and physical properties
- ASTM F963 Standard Consumer Safety Specification for Toy Safety

These safety requirements were designed for traditional toys and outline primarily physical safety hazards (e.g. mechanical hazards, electrical hazards, etc.). Electric toys have specific safety standards as well, and must meet the requirements as set out in Canadian Standards Association Standard C22.2 No. 149-1972, *Electrically Operated Toys*, (Section 5 of the *Toys Regulations*). While safety concerns concentrate primarily on physical safety limited to the physical design of the toy, privacy is not a topic widely addressed in the toy industry. Safety is a concern related to privacy when a breach of privacy can result in physical harm to the child. Physical threats to safety as a result of privacy breach can include exploitation, stalking, physical harm that can happen as a result of the knowledge of a child's location. Current toy safety regulations are not up to date and do not acknowledge the possibility of this type of safety threat.

3.3.3.2 Industry Guidelines and Best Practices

While technology continues to change, there are limitations on privacy laws and many countries and states struggle to keep up with the changing environment. Privacy related to location information, child users, and responsible marketing to children have been emerging topics in recent years. In order to help regulate this, several regulating organizations have provided guidelines and recommendations for industry *self-regulation* of the management of children's data online and mobile environments. The International Telecommunication Union (ITU) and United Nations Children's Fund (UNICEF) have released guidelines for child online protection, stressing that companies in states which lack adequate legal frameworks for the protection of children's rights to privacy and freedom of expression should follow enhanced due diligence to ensure policies and practices are in line with international law [13]**.** The guidelines encourage companies to adopt the highest privacy standards when it comes to collecting,

processing and storing data from or about children [13]. Further, services directed at or likely to attract a main audience of children must consider the risks posed to them by access to, or collection and use of, personal information (including location information), and ensure those risks are properly addressed [13].

The Mobile Marketing Association (MMA) has issued a Mobile Application Privacy Policy Framework [148] to help mobile application providers to create privacy policies. This document has special considerations for location information and children. If a child has provided information without their parent's consent, the parent can contact the provider to delete the information. The CTIA recommends Best practices and Guidelines for location based services [149] which follow closely with the privacy principles. This document does not appear to have much entirely unique for location information, but there are a couple notable items. The CTIA outlines that user's location information should be retained by LBS providers only as long as required by business needs, after which time it must be destroyed. If location must be retained for long-term use it should be converted to aggregate or anonymized data. The importance of the protection of minors is also elaborated by the CTIA regarding the use and disclosure of location information. The Digital Advertising Alliance (DAA) has also issued a report on the Application of Self-Regulatory Principles to the Mobile Environment [150]. The focus of this report is on transparency and control, and includes special considerations for "Precise Location Data."

The North American Toy Industry Association (TIA) released a whitepaper [138] regarding the changing privacy and data security landscape the toy industry is facing with the emerging popularity of child-directed mobile apps. The TIA iterates the issues of children's marketing and privacy in this context, indicating that privacy and data security issues affect day to day operations of toy companies. The TIA offers the following concerns:

- The FTC's restrictions on third party sharing, except where information is used to support the internal functions of the website, could restrict routine use of web

analytics and other activities currently permitted under the existing rule. The proposed rule affirms that COPPA applies to all online services directed to children, including mobile apps.

- Toy companies support parental authority and strive to offer children interactive, anonymous experiences under the current COPPA framework.
- Self-regulation provides an effective means of protecting children's privacy; intrusive oversight will undercut the effectiveness.

3.4 Privacy Requirements for Toy Computing

In this analysis for privacy in a toy computing environment, there were several factors to take into consideration regarding the privacy goals based on our threat model, end user requirements, laws and regulations. In this section we present the requirements for a privacy framework based on these factors. Data minimization and user participation are privacy goals based on our threat model. A framework is required which can achieve these privacy goals by minimizing the collection and retention of potentially sensitive user data, as well as involving the user (or parent) in the control of their child's data. End user requirements need to consider that the main user base is children, who have unique requirements as they are especially vulnerable and in order to protect their sensitive location data, parents/guardians require a method to implement privacy controls on their child's data. Next, the framework must help to achieve the 10 principles of privacy and comply with PIPEDA.

3.4.1 Six Privacy Constraints for Toy Computing

Based on the above, we have compiled 6 privacy rights for parents/guardians to have control over their child's location data in toy computing. These privacy requirements enforce the goals of data minimization and user participation, by allowing parents/guardians to be in control of how their child's privacy is managed, and restrict the data that is collected. These requirements comply with the 10 principles of privacy of which PIPEDA is based.

1. **The right for a parent/guardian to request restrictions on the use or disclosure of private information of their child.** This allows parents/guardians to provide restrictions to purpose, recipients, obligations, and retention regarding their child's location information. This protects children from having their location information being used or shared for any purpose considered illegitimate or unacceptable to the parent/guardian.
   - *Goals*: user participation, data minimization
   - *Privacy Principles*: consent, limiting collection, limiting use disclosure and retention
2. **The right for a parent/guardian to access, copy, and inspect collected records on their child**. This allows a parent/guardian to access their child's location records to see that data that is collected on them.
   - *Goals*: user participation
   - *Privacy Principles*: access
3. **The right for a parent/guardian to request deletion of their child's private data records, or correction if records are inaccurate**. This allows parents/guardians to request that their child's location records be deleted, or to request a correction if their child's location records are incomplete or incorrect.
   - *Goals*: user participation, data restriction
   - *Privacy Principles*: limiting collection & retention, accuracy, access
4. **The right for a parent/guardian to request acknowledgements through a communication channel when private information of their child is collected.** This allows parents to set up a communication channel such as phone number or email address to receive acknowledgements there is an update pertaining to the collection of their child's location records. This allows parents/guardians to keep track of how their child's location information.
   - *Goals*: user participation
   - *Privacy Principles*: openness, access

5. **The right to file complaints to toy company**. If a parent/guardian believes that their child's data has been mishandled in any way by the toy company or service provider, or if they believe that they have not acted in compliance with their policies, they are able to file complaints.
    - *Goals*: user participation
    - *Privacy Principles*: accountability, challenging compliance
6. **The right to find out where the child's private data has been shared for purposes other than a game.** This allows a parent/guardian to be notified if their child's location records have been shared with another party for any purpose other than for a game.
    - *Requirements*: user participation
    - *Privacy Principles*: notice, purpose, openness

3.5 Chapter Summary

This chapter outlines the privacy requirements and concerns that parents and children observe in a mobile toy computing environment. We provide an overview of privacy issues, and next present a privacy threat model illustrating the privacy threats and requirements in a toy computing environment. Next we investigate the privacy considerations related to children as the primary user base and the issues parents face for implementing privacy controls. Additionally, we examine the privacy laws and regulations related to children's online and mobile privacy and toy computing. Finally, based on these requirements we present six privacy constraints as a basis for the privacy access control model in Chapter 4.

Chapter 4 **Privacy Access Control Model**

In this chapter we developed an access control model with the concepts of toy, mobile services, devices, and guidance with related privacy entities: purpose, recipient, obligation, and retention for the toy computing environment. In this model, the parents/guardians are the owners of the data which is collected on their child (the data subject). Parents/guardians provide consent through access rules which allow their child's data to be shared according to their preferences and privacy compliance.

4.1 Core Access Control Model

In the core access control model, a subject is a 3-tuple entity comprised of a toy, a device, and a mobile service. The mobile service may communicate with external entities over a network, such as other devices or Web services. The user who interacts with the subject is a child (data subject) who is associated with a real identity and a parent/guardian (data owner) who is in control of their data. For the purpose of this work we will use the same definition as SEC. 1302 of the US Children's Online Privacy Protection Act (COPPA) [23], which defines a "child" as an individual under the age of 13 years old. In this model access control decisions are based on permissions which are assigned by the parent, comprised of a list of rules for operations (read, write, etc.), and objects. Figure 4.1 illustrates the core access control model which allows parents to manage their privacy preferences for access to their child's location data. The entities and properties of this model will be described in more detail in the following sections.

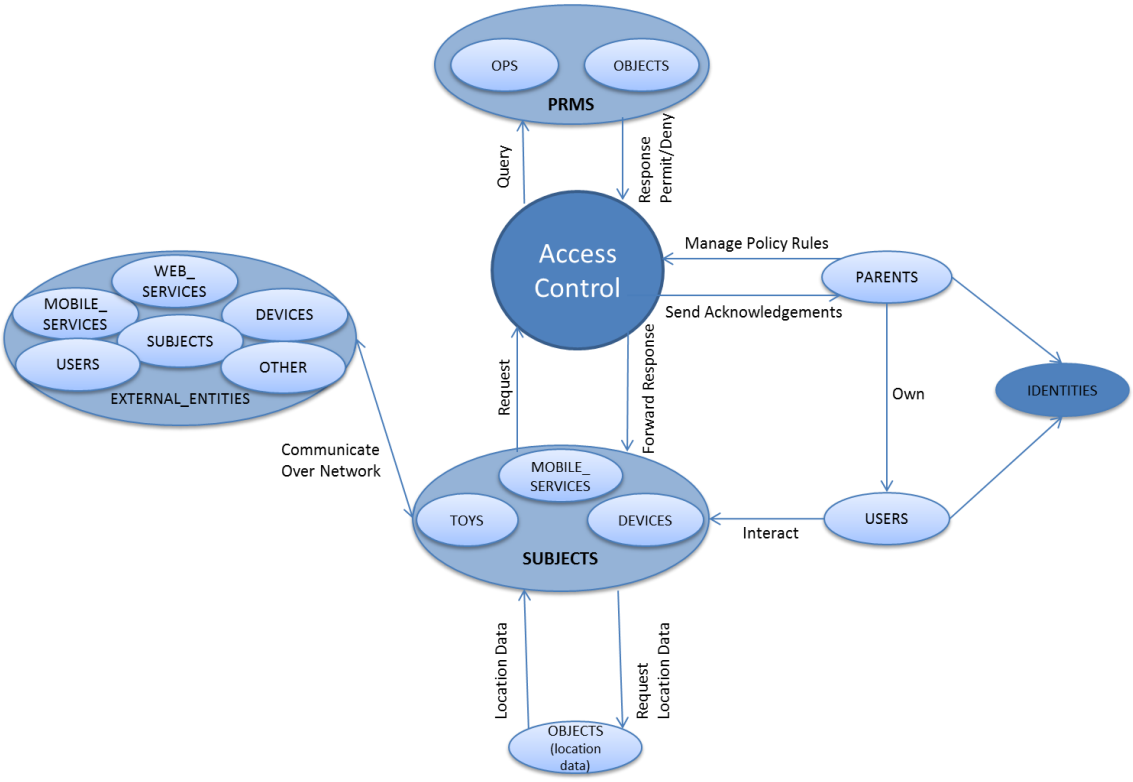

Figure 4.1 Core Access Control Model

4.1.1 Definitions

- **TOYS = {to_1, to_2, …, to_l}** is a set of *l* toys in the system, where *l* > 0. As defined in Chapter 1, a toy is a physical object designed for play in a toy computing environment.
- **DEVICES = {d_1, d_2, …, d_m}** is a set of *m* mobile devices in the system, where *m* > 0. A mobile device is a smartphone or tablet PC.
- **MOBILE_SERVICES = {ms_1, ms_2, …, ms_n}** is a set of *n* mobile services in the system, where *n* > 0. Mobile services communicate with mobile devices to provide services to run the toy computing game environment. Mobile services may request location or other data from the user u.
- **SUBJECTS = {s_1, s_2, …, s_p}** is a set of *p* subjects in the system, where p > 0. A subject *s* is a 3-tuple s = (to_i, d_j, ms_k), where to_i ∈ TOYS, d_j ∈ DEVICES and ms_k ∈ MOBILE_SERVICES. These entities are grouped together to form a subject because they are the core entities that comprise the toy computing system.

- **USERS = {u_1, u_2, …, u_q}** is a set of *q* users in the system, where *q* > 0. Users are children aged 13 years or younger, based on [23].
- **PARENTS = {pg_1, pg_2, … pg_r}** is a set of *r* parent/guardians in the system, where *r* > 0.
- **IDENTITIES = {id_1, id_2, … id_t}** is a set of *t* real identities in the system, where *t* > 0. A real identity is the actual identity of the user or parent/guardian and can be used to identify them outside of the system (e.g. name, address, phone number).
- **EXTERNAL_ENTITIES = {e_1, e_2,…e_u}** is a set of *u* external entities *e*, where *u* >= 0. External entities include external mobile services, Web services, servers, users, devices, etc. to which mobile services can connect and interact with over a network. External entities are listed under RECIPIENTS in a service's policies, which will be detailed more in a later section.
- **OBJECTS = {o_1, o_2,…, o_g}** is a set of *g* objects in the system, where *g* > 0. In this research work, objects are mainly location data.
- **OPS = {op_1, op_2, …, op_h}** is a set of *h* operations in the system, where *h* > 0. This research mainly focuses on the *read* operation, i.e. **OPS = {read}**.
- **PRMS = $2^{(OPS * OBJECTS)}$** is a set of permissions in the system that approves a particular operation on one or more objects.

4.1.2 Properties

- ***parent_user:*** **(pg: PARENTS) → (u: USERS)** is a 1-to-*n* mapping of a parent/guardian *pg* to a user *u* who is their child. A parent/guardian can have multiple children.
- ***user_parent:*** **(u: USERS) → (pg: PARENTS)** is a 1-to-1 mapping of a child user *u* to their parent/guardian. A child can only have one parent/guardian.
- ***user_identity*****: (u: USERS | pg: PARENTS) → (id: IDENTITIES)** is a one-to-one mapping of a user *u* or parent/guardian *pg* to their real identity *id*.
- ***subject_user*****: (s: SUBJECTS) → (u: USERS)** is a one-to-one mapping of a subject *s* onto an associated user *u*. When the user (child) is engaged in with the subject s in a toy computing environment, the 3-tuple subject: (toys, mobile device, mobile services) is associated with that user.

- ***toy_device*: (to: TOYS) → (d: DEVICES)** is a one-to-*n* mapping of a toy to onto an associated device *d*. Toys may have a list of related mobile apps (one-to-n mapping). Toys cannot run without a mobile device.
- ***toy_service: (to:* TOYS*) → (ms:* MOBILE_SERVICES*)** is an *n*-to-*n* mapping of a device *d* onto an associated mobile service *ms*. Toys cannot run without a mobile service attached with a device.
- ***device_service*: (d: DEVICE) → (ms: MOBILE_SERVICES)** is an *n*-to-*n* mapping of a device *d* onto an associated mobile service *ms*. A toy can be mapped to multiple mobile services and vice versa.
- ***subject_entities: (s:* SUBJECTS*) → (e:* EXTERNAL_ENTITIES*)** is a one-to-*n* mapping of a subject *s* to a set of external entities $\{e_1, e_2, \ldots, e_u\}$ they are connected to over a network, for example, a multi=player game.
- ***assigned_permissions: (s:* SUBJECTS*) →* 2^{PRMS}** is a one-to-many mapping of a subject *s* to its associated permissions.

Privacy-Sensitive Properties:

- ***Child_location: (id: IDENTITIES) → (o: OBJECTS)*** is a one-to-many mapping of a child's real identity *id* to the objects *o* they are associated with (i.e. location). In the toy computing environment, location data is particularly sensitive data because it is the location of the child using the toy. The location object is sensitive information when associated with the user's real identity because it allows other entities to be aware of the child's physical location. The motivation for this access control model is to protect this property from being shared with untrusted external entities.

4.2 Privacy Access Control Model

Traditional access control models make access decisions (permit/deny) based on low level operations, such as read and write, for describing a subject's operation on an object. For example, user A is allowed to read file B, in which case user A is the subject, file B is the object, and *read* is the operation.

Figure 4.2 presents an extended access control model for privacy in a toy computing environment. This model shows the privacy access control model extended over top of the core access control model discussed in the previous section. In the privacy access control model, a request <*Subject, Operation, Object, Purpose(s), Recipient(s)*> as input, and a response <*Decision, Obligation(s), Retention*> as output, as well as an optional acknowledgement <*Subject, Event*> through a communication channel.

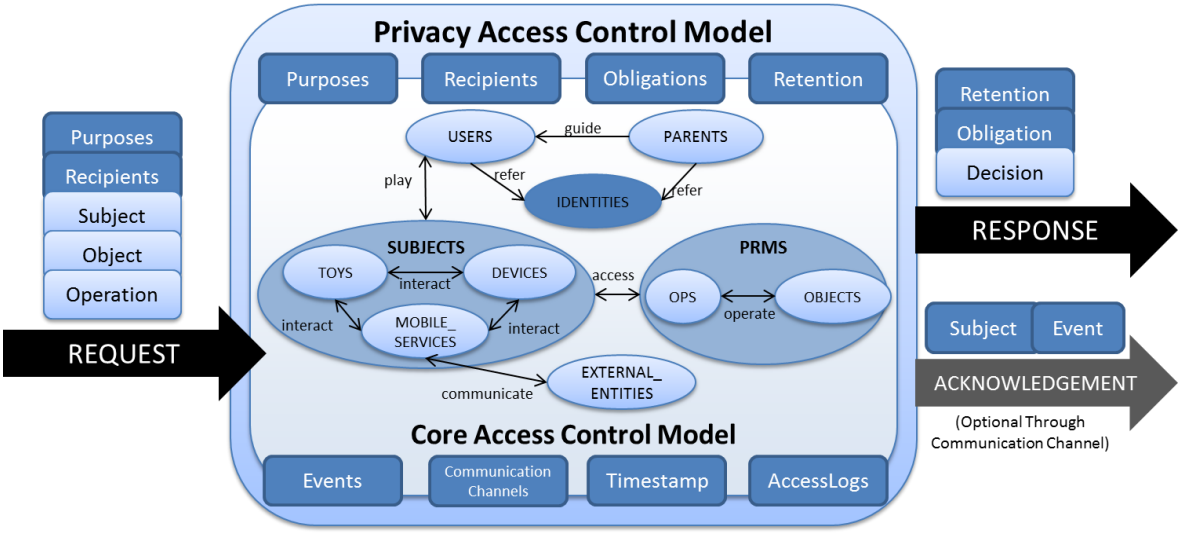

Figure 4.2 Extended Privacy Access Control Model

- ***Request*** is a 5-tuple <*Subject, Operation, Object, Purpose(s), Recipient(s)*>. It is an input for the privacy access control model.
- ***Privacy Access Control Model*** consists of a core access control model, privacy-based entities (*Purposes, Recipients, Obligations, Retention*), and other entities (*Events, CommunicationChannels, Timestamp, AccessLogs*). The model processes an input request and generates a corresponding response, and an optional acknowledgement through a predefined communication channel.
- ***Response*** is a 3-tuple <*Decision, Obligation(s), Retention*>, as an output of the model with a decision along with a set of obligations and retention policy for permitted access.

- ***Acknowledgement*** is a 2-tuple <*Subject, Event*>, which is an optional output of the model to send an acknowledgement of the event to a subject's corresponding parent/guardian via a predefined communication channel.

4.2.1 Privacy-Based Entities

In our extension for preserving privacy, we have proposed four privacy-based entities: PURPOSES, RECIPIENTS, OBLIGATIONS, and RETENTION based on P3P [93]. These privacy-based entities are described as follows:

- **PURPOSES = {pp_1, pp_2, …, pp_n}** is a set of *n* purposes in the system. A subject must specify a set of purposes in the corresponding access request. A purpose can be described as different sub-purposes or combined into a "general" purpose in a hierarchical structure [151]. Figure 4.3 shows an example hierarchical structure to represent different purposes that could be related to toy computing. Different purposes can be generalized as the root element "AnyPurpose," which is the most general purpose in the system. "AnyPurpose" can further be sub-classified as "PersonalPurpose," "MarketingPurpose," "AdministrativePurpose," "GamePurpose" and "ResearchPurpose." Each of these can further be sub-classified into more specific purposes. Please note that handling purpose hierarchy is outside the scope of this thesis.

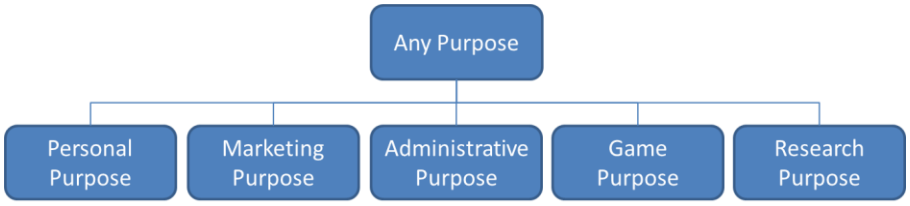

Figure 4.3 Purpose Hierarchy

- **RECIPIENTS = {rp_1, rp_2, …, rp_n}** is a set of *n* recipients of the collected object(s) belonging to the subjects/users in the system. Each collected object has a corresponding set of recipients. In the context of toy computing and P3P, recipients can be described as one of the following categories:

- ***Individual**:* The subject who made the request or an individual USER or SUBJECT in the system.
- ***Group**:* a group of users (e.g. the group of USERS or SUBJECTS currently engaged in a toy computing game session).
- ***Third-Party***: an entity which does not belong to the system, but is constrained by and accountable to the object owner. This includes EXTERNAL_ENTITIES.
- ***Anyone**:* Any subject or external entity.

- **OBLIGATIONS = {obl_1, obl_2, …, obl_n}** is a set of *n* obligations of in the system that is necessary to be accepted after access permission is granted. The obligations describe the rules that a subject agrees to comply with after gaining the access permission. Obligations are generally bound to legislation and agreements, for example, "No disclosure to an unauthorized third party."
- **RETENTIONS = {rt_1, rt_2, …, rt_n}** is a set of *n* retention policies in the system to be enforced after permission is granted. Each object may have a corresponding retention policy to enforce the duration for how long it may be used or retained. It is recommended that a child's location data be retained only for the time necessary for the stated purpose. Based on the context of P3P [93], the retention policy can be described as one of the following categories:
  - *No-retention:* the requested object is not retained for more than a brief period of time, after which it must be destroyed without being logged, archived or otherwise stored by the recipients.
  - *Stated-purpose*: the requested object is retained for the time required to meet the stated purpose and will be discarded as soon as possible after the purpose is satisfied.
  - *Legal-requirement:* the requested object is retained to meet a stated purpose (as required by law or liability under applicable law).
  - *Business-practices:* the requested object is retained under the stated business practices.

- *Indefinitely*: the requested object is retained for an indeterminate period of time.

4.2.2 Other Related Entities

- ***DECISIONS* = {*permit, deny*}** is a Boolean value for an access permitted or denied decision e.g. permit = TRUE and deny = FALSE.
- ***PRIVACY_RULES* ⊆ *SUBJECTS* x *USERS* x *OPS* x *OBJECTS* x *PURPOSES* x *RECIPIENTS* x *DECISIONS* x *OBLIGATIONS* x *RETENTIONS*** is a set of privacy rules in the system. For a positive authorization rule (*DECISIONS* = *permit*), the rule states what subject is allowed to perform which operation on which object for what purposes, to which recipients, and under what obligations and retention.
- ***CHILD_DATA* ⊆ *SUBJECTS* x *OBJECTS* x *USERS*** is a one-to-many mapping between child users, the subjects they interact with, and the objects belonging to them. It is a 3-tuple <s,o,u> where s ∈ SUBJECTS, o ∈ OBJECTS, and u ∈ USERS. This is all of the data associated with a child during their interactions with toy computing.
- ***OWNERS* ⊆ *PARENTS* x *[SUBJECTS* x *OBJECTS* x *USERS]*** is a one-to-many mapping between parents pg and child data (subject s, object o, and user u,). It is a 4-tuple <pg, s,o,u>, where pg ∈ PARENTS, s ∈ SUBJECTS, o ∈ OBJECTS, u ∈ USERS, and <s,o,u> ∈ CHILD_DATA. The set of owners in the system refers to whom the object belongs. In the case of mobile toy computing, the owner of a child's data is the child's parent/guardian.
- ***COMMUNICATION_CHANNELS* = {c_1, c_2, …, c_n}** is the set of communication channels in the system. It is used to specify how the acknowledgement is sent to a parent/guardian, for example, email, phone, etc.
- ***TIMESTAMP*** is a set of positive integers Z^+, representing the system time in partial order.
- ***ACCESS_LOGS* = {e_1, e_2, …, e_n}** is a set of *n* events to keep track of access control log history of all events occurred in the system. Initially, the system has an empty access log, which is populated as events occur. *EVENTS* are all possible incidents that occur in the system. An event contains a *TIMESTAMP* attribute to record the system time

when the event occurred. All events that occur in the system are stored in *ACCESS_LOGS* ⊆ *EVENTS*, which are classified into four different types:

- EVENTS ⊆ *SUBJECTS x USERS x OPS* x *OBJECTS* x *PURPOSES* x *RECIPIENTS* x *DECISIONS* x *OBLIGATIONS* x *RETENTIONS* x *TIMESTAMP* is an event of an access request and the corresponding response.
- EVENTS ⊆ *PARENTS x ACCESS_LOGS* x *TIMESTAMP* is an event of an acknowledgement.
- EVENTS ⊆ *SUBJECTS x PRIVACY_RULES* x *PRIVACY_RULES* x *TIMESTAMP* is an event of a change in privacy rules or restrictions.
- EVENTS ⊆ *PARENTS x COMMUNICATION_CHANNELS* x *TIMESTAMP* is an event of a change in an acknowledgement communication channel.

- ***OBJECT_TYPES = {type₁, type₂, …, typeₙ}*** is a set of *n* types of categories of objects. While we are concerned with location data, some relevant categories are as follows, as illustrated in Figure 4.4.
  - *AnyLocationObjectType*: a general description of any location object type.
  - *Absolute Location*: is the location expressed in a range or exact GPS coordinates, latitude and longitude. For the purpose of this thesis, we are concerned with absolute location. As defined in Chapter 2, the absolute location can be expressed as coarse (GPS-based, approximate location), or fine (network-based, precise location) [61].
  - *Relative Location*: is the location relative to another entity as a reference point. Relative location can be expressed as the distance between User A and User B, User A and Device C, or User A and Location D.
  - *Type of Location*: is the location expressed in a predefined category. Some examples include home, office, street, mall, or restaurant.

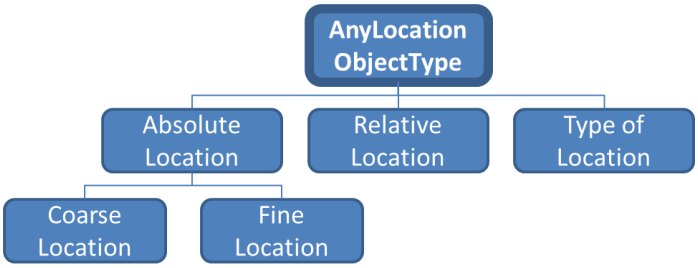

Figure 4.4 Location Object Types

4.2.3 Extended properties

- **object_user: (o: OBJECTS) → (u: USERS, s: SUBJECTS)** is a mapping of a child's data object, onto its associated user u. Formally, object_user(o) = <*s, o, u*> where <*s, o, u*> ∈ CHILD_DATA.
- **user_objects: (u: USERS) → $2^{OBJECTS}$** is a one-to-many mapping of a user u to all of the objects o it is associated with. Formally, user_object(u) = { <s,*o,u*>$_1$, <s,*o,u*>$_2$, …, <s,*o,u*>$_n$}, where *o* ∈ *OBJECTS, s* ∈ *SUBJECTS, , u* ∈ *USERS* and <s,*o,u*> ∈ CHILD_DATA.
- ***object_owner:*** **(o: OBJECTS) → (pg: PARENTS)** is a mapping of a child data <s,*o,u*> onto its owner (i.e. parent pg). Formally, *object_owner(o)* = (pg, <s,*o,u*>) where (pg, <s,*o,u*>) ∈ OWNERS.
- ***owner_objects:*** **(pg: PARENTS) →$2^{OBJECTS}$** is a mapping of a parent/guardian to all of the objects that the parent/guardian owns. Formally, *owner_objects(pg)* = {(pg, <s,*o,u*>)$_1$, (pg, <s,*o,u*>)$_2$, …, (pg, <s,*o,u*>)$_n$ } where (pg, <s,*o,u*>) ∈ *OWNERS.*
- ***type:*** **(*o: OBJECTS*) → (*oType: OBJECT_TYPES*)** is a one-to-one mapping of an object *o* to its object type *oType*. Each object is associated with an object type in the *LocationObjectType* categories, which belongs to *OBJECT_TYPES*.
- ***restrict:*** **(rule1: PRIVACY_RULES) → (*rule2: PRIVACY_RULES)*** is a one-to-one mapping to map *rule1* onto *rule2* that both *rule1* and *rule2* are elements of *PRIVACY_RULES*. This is used to restrict the privacy rules by specifying the purposes, recipients, obligations, and retention for an access.
- ***comm_channel:*** **(pg*: PARENTS) → (c: COMMUNICATION_CHANNELS)*** is a one-to-one mapping to map parent/guardian pg onto his/her communication channel *c*. This is used to determine how an acknowledgement is sent through a communication medium such as email or telephone. Communication channels are

available to a child user's parents/guardians if they wish to receive acknowledgements.

- ***acknowledgement:*** **(pg ∈ PARENTS**, ***c ∈ COMMUNICATION_CHANNELS, e ∈ ACCESS_LOGS*****) → BOOLEAN** is a notification mechanism to a parent/guardian pg corresponding to an event e that occurs in the system. The acknowledgement should be sent through a communication channel c defined by the parent/guardian. If the parent/guardian has setup an acknowledgement communication channel, the function will return TRUE. If the parent/guardian has not setup an acknowledgement communication channel, or opted not to receive any acknowledgement, the function will return FALSE.
- ***log:*** **(e: EVENTS) → ACCESS_LOGS** is a one-to-one mapping of an instance of an event *e* that occurs in the system onto an audit trail ACCESS_LOGS. When an event occurs, the ACCESS_LOGS will keep a record of the related details of the event. Formally, *log*(*e*) = *ACCESS_LOGS* ∪ *e*.

4.3 Access Control Authorization Properties in the Model

4.3.1 Basic Access Authorization Property

- *basic_access: SUBJECTS* x *OPS* x *OBJECTS* → *DECISIONS*
- *basic_access(s, op, o)* = *permit* if subject *s* can access object *o* using operation *op,*

  = *deny* otherwise.

  A subject s is permitted to perform an operation *op* on object *o* only if there exists a permission assigned to *s* such that the permission authorizes the performance of *op* on *o*:

  s ∈ *SUBJECTS, o* ∈ *OBJECTS, op* ∈ *OPS,*

  basic_access(s, op, o) = *permit*

  ∃ *s: SUBJECTS, p: PRMS,*

  $p \in assigned\_permissions(s) \wedge (op,o) \in p$

4.3.2 Privacy Access Authorization Property

- ***privacy_access:*** **SUBJECTS|PARENTS x USERS x *OPS* x *OBJECTS* x *PURPOSES* x *RECIPIENTS* → *DECISIONS* x *OBLIGATIONS* x *RETENTIONS***. Based on the *PRIVACY_RULES*, the privacy access is used to determine whether a privacy access is permitted or denied with related obligation(s) and a retention policy is returned. This takes into account the object, user, and subject who invokes access, the operation, the purpose(s) for the request, and the recipient(s) of the collected object.
- ***privacy_access (pg, u, op, o, _, _) ,*** *where user is parent's child, operation is read,* ***= (permit, _, _).*** *Parents have the right to access their child's objects without any restrictions.*
- ***privacy_access (s, u, op, o, {pp_1, pp_2,…,pp_j}, {rp_1, rp_2, …, rp_k})***
  = (permit, {obl_1, obl_2, …,obl_m}, rt) if and only if: (*s, u, op, o, {pp_1, pp_2,…,pp_j}, {rp_1, rp_2, …, rp_k}, permit, {obl_1, obl_2, …,obl_m}, rt)* ∈ *PRIVACY_RULES*
  A subject can access an object *o* using an operation *op* for a set of purposes in *{pp_1, pp_2,…,pp_j}* to a set of recipients in *{rp_1, rp_2, …, rp_k}*, and following a set of obligations in *{obl_1, obl_2, …,obl_m}* and a retention policy *rt*.

  = (*deny*, ∅, ∅) if and only if there is no match in the privacy rule or there is a *deny* rule: (s*, u, op, o, {pp_1, pp_2,…,pp_j}, {rp_1, rp_2, …, rp_k}, deny,* ∅, ∅) ∈ *PRIVACY_RULES*

4.4 Privacy Constraints

In Chapter 3, we defined a set of privacy requirements for toy computing based on PIPEDA and toy safety guidelines. In this section, we interpret the privacy requirements as constraints in the extended access control model and illustrate the constraint rules. Constraints are used to specify the specific requirements that need to be enforced in the system. The toy computing privacy requirements are presented as the following constraints:

- **Constraint 1**: The right for a parent/guardian to request restrictions on the use or disclosure of private information of their child.
- **Constraint 2**: The right for a parent/guardian to access, copy, and inspect collected records on their child.
- **Constraint 3**: The right for a parent/guardian to request deletion or correction if records are inaccurate.
- **Constraint 4**: The right for a parent/guardian to request acknowledgements through a communication channel when private information of their child is collected.
- **Constraint 5**: The right to file complaints to toy company.
- **Constraint 6**: The right for a parent/guardian to find out where private data has been shared for purposes other than a game.

4.4.1 Constraint 1: The right to for a parent/guardian to request restrictions on the use or disclosure of private information of their child

Description: the set of privacy rules in the system is (a) updated, (b) acknowledged, and (c) logged if and only if (1) a parent/guardian pg applies a restriction on his/her child's object o, and (2) the restrictions include a set of purposes; a set or recipients; a set of obligations and a retention policy on a mobile service (subject s) to perform an operation op on object o:

$\forall s \in SUBJECTS, u \in USERS, op \in OPS, o \in OBJECTS, pg \in PARENTS$

$PP, PP' \subseteq PURPOSES, RP, RP' \subseteq RECIPIENTS, OBL, OBL' \subseteq OBLIGATIONS,$

$rt, rt' \in RETENTIONS, rule \in PRIVACY\_RULES$

$pg \in user\_parent(u) \wedge u \in object\_user(o) \Rightarrow pg \in object\_owner(o)$ (1)

$\wedge rule = (s, u, op, o, PP, RP, permit, OBL, rt),$

$\wedge (PP \neq PP' \vee RP \neq RP' \vee OBL \neq OBL' \vee rt \neq rt')$

$\wedge restrict(s, u, op, o, PP, RP, OBL, rt) = (s, u, op, o, PP', RP', OBL', rt')$ (2)

⇒

∃ c ∈ COMMUNICATION_CHANNELS, t ∈ TIMESTAMP, e ∈ EVENTS,

rule’ = (s, u, op, o, PP’, RP’, permit, OBL’, rt) ∈ PRIVACY_RULES,

PRIVACY_RULES = PRIVACY_RULES /rule,

PRIVACY_RULES = PRIVACY_RULES ∪ rule’, (a)

e = (s, rule, rule’, t), c = com_channel(object_owner(o)),

acknowledgement(object_owner(o), c, e), (b)

log(e) (c)

Proof: The proof consists of two parts, (i) showing Constraint 1 is necessary, and (ii) showing Constraint 1 is sufficient.

Constraint 1 is necessary according to our privacy rule 1, that a parent/guardian has the right to request restrictions on the use or disclosure of the location information of their child. Therefore, the parent/guardian has the right to setup restrictions on the access purposes, recipients, obligations, and retention of the location data of their child. Therefore a set of privacy rules in the system governing the access of object o is updated if an only if the parent/guardian pg applies a restriction on his/her child’s object. The restrictions include a set of purposes; a set of recipients; a set of obligations and a retention policy on a subject which performs an operation op to object o.

To show that Constraint 1 is sufficient, we know that every parent/guardian pg owns a set of objects belonging to their child owner_object(pg), where $0 \leq |\text{owner\_objects(pg)}| \leq n$ and $n \geq 1$. For owner_objects(pg) = ∅, the parent/guardian pg does not have any permission right to request update of any restrictions on any private information. For owner_objects(pg) ≠ ∅, the parent/guardian pg would be granted the right to make a restriction request on object o which belongs to owner_objects(pg) only. Before the restriction request at time t, the privacy policy states that when any subject

performs an operation op on object o with the purposes PP and recipients RP, it is permitted with obligations OBL and retention policy rt. In the system, there may be events which occur at t' where t' ≤ t, 0 ≤ |e| where e = (s, u, op, o, PP, RP, permit, OBL, rt, t') for any subject s. After the update of privacy rules at time t, the privacy policy states that any when subject performs an operation op on object o with the purposes PP' and recipients RP', it is permitted with obligations OBL' and retention policy rt'. The privacy access rules in the system are thus updated with a deletion of an entry (s, u, op, o, PP, RP, permit, OBL, rt), and an insertion of an entry (s, u, op, o, PP', RP', permit, OBL', rt') in the system privacy policy. Therefore, after time t, the access logs must not contain any event such as: ¬(∃e = (s, u, op, o, PP, RP, permit, OBL, rt, t')) where t' > t.

4.4.2 Constraint 2: The right for a parent/guardian to access, copy and inspect collected private records on their child

Description: The privacy access is (a) allowed, (b) acknowledged, and (c) logged if and only if, a parent/guardian exists (1) to perform an operation "read" or "copy" (2) to his/her own child's object *o* which is a type of "AnyLocationObjectType."

∀ s ∈ SUBJECTS, u ∈ USERS, op ∈ OPS, o ∈ OBJECTS, pg ∈ PARENTS

∧ op = ("read" ∨ "copy") (1)

pg ∈ user_parent(u) ∧ u ∈ object_user(o) ⇒ pg ∈ object_owner(o)

∧ o ∈ owner_object(pg) ∧ type(o) = "AnyLocationObjectType" (2)

⇒

∃ c ∈ COMMUNICATION_CHANNELS, t ∈ TIMESTAMP, e ∈ EVENTS,

privacy_access(s, u, op, o, _, _) = (allow, _, _), (a)

e = (s, u, op, o, _, _, allow, _, _, t), c = com_channel(object_owner(o)),

acknowledgement(object_owner(o), c, e), (b)

log(e) (c)

Proof: the proof consists of two parts: i) showing Constraint 2 is necessary, and ii) showing Constraint 2 is sufficient.

Constraint 2 is necessary according to our privacy constraint 2, that a parent/guardian has the right to access, copy, and inspect collected location records on their child. Therefore, the privacy access is allowed, acknowledged, and logged if a parent/guardian pg requests an operation "read" or "copy" to his/her child's own object o which is a type of "AnyLocationObjectType."

To show that Constraint 2 is sufficient, we know that every parent/guardian pg owns a set of objects owner_object(pg), where $0 \leq |\text{owner\_objects(pg)}| \leq n$ and $n \geq 1$. For owner_objects(pg) = ∅, the parent/guardian pg does not have permission to access, inspect, or copy any location records. For owner_objects(pg) ≠ ∅, the parent/guardian pg may also have no permission to access, inspect, and copy his/her child's location records if and only if $\neg(\exists\, o \in \mathit{owner\_objects}(\mathit{pg}) \Rightarrow \mathit{type}(o) =$ "AnyLocationObjectType"). Thus, the parent/guardian pg can only have permission to access, inspect, and copy his/her child's medical records ($o \in \mathit{owner\_objects}(\mathit{pg}) \mid \mathit{type}(o) =$ "AnyLocationObjectType" ∧ owner_objects(pg)) ≠ ∅). When the parent/guardian pg acquires the access permission, this event e will be logged and stored in the system. If the object owner (parent pg) has set up an acknowledgement channel c, an acknowledgement of the event e will be sent via c.

4.4.3 Constraint 3: The right to request deletion or correction if private records are inaccurate or unwanted

The correction of location records action corresponds to the action "correct" in the system. The operation "correct" means that there is a trusted third party to update the information for the subject.

Description: the privacy access is (a) allowed, (b) acknowledged, and (c) logged, if and only if a parent/guardian pg is (1) permitted to perform an operation "correct" or

"delete" (2) to his/her child's own object o which is a type of "AnyLocationObjectType" (3) for the purpose of "CorrectInaccurateLocation" or "DeleteUnwantedLocation."

$\forall$ s $\in$ SUBJECTS, u $\in$ USERS, op $\in$ OPS, o $\in$ OBJECTS, PP $\in$ PURPOSES, pg $\in$ PARENTS

pg $\in$ parent_user(u) $\wedge$ u $\in$ object_user(o) $\Rightarrow$ pg $\in$ object_owner(o)

$\wedge$ op = ("correct"|"delete") (1)

$\wedge$ o $\in$ owner_object(pg) $\wedge$ type(o) = "AnyLocationObjectType" (2)

$\wedge$ PP = ("CorrectInaccurateLocation"|"DeleteUnwantedLocation") (3)

$\Rightarrow$

$\exists$ c $\in$ COMMUNICATION_CHANNELS, t $\in$ TIMESTAMP, e $\in$ EVENTS,

privacy_access(pg, u, op, o, PP,_) = (permit, _, _), (a)

e = (s, u, op, o, PP, _, permit, _, _, t), c = com_channel(object_owner(o)),

acknowledgement(object_owner(o), c, e), (b)

log(e) (c)

Proof: the proof consists of two parts: i) showing Constraint 3 is necessary, and ii) showing Constraint 3 is sufficient.

Constraint 3 is necessary according to our privacy rule 3, that a parent/guardian has the right to request the correction of any inaccurate location information or deletion of any unwanted location information pertaining to their child. Therefore, the privacy access is allowed, acknowledged, and logged if a parent/guardian pg requests an operation "correct" on his/her own object o for the purpose of "CorrectInaccurateLocation" or "DeleteUnwantedLocation."

To show that Constraint 3 is sufficient, we know that every parent/guardian pg owns a set of objects owner_object(pg), where $0 \leq |\text{owner\_objects(pg)}| \leq n$ and $n \geq 1$. For

owner_objects(pg) = ∅, the parent/guardian pg does not have any permission to correct or delete any location records. For owner_objects(pg) ≠ ∅, the parent/guardian pg would be granted the right to make a correction request on any of his/her own child's objects o ∈ owner_objects(pg) with the type of "AnyLocationObjectType" which belongs to owner_objects(pg) with the purpose "CorrectInaccurateLocation" or "DeleteUnwatnedLocation." Thus, the parent/guardian pg can only have a permission to correct his/her own child's location records (of which they are the parent/guardian is the owner): (o ∈ $owner\_objects(pg)$ | $type(o)$ = "AnyLocationObjectType" ∧ $owner\_objects(pg)$ ≠ ∅ ∧ PP = {"CorrectInaccurateLocation" | "DeleteUnwantedLocation"}). When the parent/guardian pg acquires the access permission, this event e will be logged and stored in the system. If the object owner (parent pg) has set up an acknowledgement channel c, an acknowledgement of the event e will be sent via c.

4.4.4 Constraint 4: The right for a parent/guardian to request acknowledgements through a communication channel when private information of their child is collected

Description: the privacy access is (a) allowed, (b) acknowledged, and (c) logged, if and only if a parent/guardian pg is (1) permitted to perform an operation "update" (2) to the parent's acknowledgement communication channel c'.

∀ pg ∈ PARENTS, op ∈ OPS, c, c' ∈ COMMUNICATION_CHANNELS,

∧ op = ("update") (1)

∧ c ∈ com_channel(pg) ∧ c ≠ c' (2)

⇒

∃ t ∈ TIMESTAMP, e ∈ EVENTS,

privacy_access(pg, u, op, _, _) = (permit, _, _), (a)

com_channel(pg) = c', e = (pg, c', t),

acknowledgement(pg, c', e), (b)

log(e) (c)

Proof: the proof consists of two parts: i) showing Constraint 4 is necessary, and ii) showing Constraint 4 is sufficient.

Constraint 4 is necessary according to our privacy Constraint 4, which iterates that the parent/guardian of the child user has the right to request communication of information privacy notification events through a specified communication channel, for example, to a particular e-mail address or phone number. Therefore, the privacy access is allowed, acknowledged, and logged if and only if a parent/guardian pg requests an operation "update" on the acknowledgement communication channel.

To show that Constraint 4 is sufficient, we know that every location record owner should receive an acknowledgement notification if any event occurs in the system. Before time t, any events in the system about object o must be sent through the communication channel c defined by the owner, where object_owner(o) = pg. For any events e which occur on object o at time t' where t' > t, the location record owner can only receive an acknowledgement notification through the acknowledgement channel c':

$\forall e = (\_, \_, o, \_, \_, \_, \_, \_, t'), e \in ACCESS\_LOGS \wedge t' \geq t$

$\Rightarrow \neg\ acknowledgement(object\_owner(o), c, e)$.

4.4.5 Constraint 5: The Right to File Complaints to Toy Company

Description: the privacy access is (a) allowed, (b) acknowledged, and (c) logged, if and only if a parent/guardian pg is (1) permitted to perform an operation "file" to a complaint record (2) on his/her own object o which is a type of "complaintRecord."

∀ pg ∈ PARENTS, u ∈ USERS, op ∈ OPS, o ∈ OBJECTS,

∧ op = ("file") (1)

∧ c ∈ owner_object(pg) ∧ type(o) = “ComplaintRecord” (2)

⇒

∃ c ∈ COMMUNICATION_CHANNELS, t ∈ TIMESTAMP, e ∈ EVENTS,

privacy_access(pg, op, o, _, _) = (permit, _, _), (a)

e = (pg, op, o, _, _, permit, _, _, t), c = com_channel(object_owner(o)),

acknowledgement(object_owner(o), c, e), (b)

log(e) (c)

Proof: the proof consists of two parts: i) showing Constraint 5 is necessary, and ii) showing Constraint 5 is sufficient.

Constraint 5 is necessary according to our privacy constraint 5, that a parent/guardian has the right to complain to the toy company regarding how they handle their child’s location data. Therefore, the privacy access is allowed, acknowledged, and logged if and only if subject s performs an operation “file” on the complaint record that the parent/guardian owns.

To show that Constraint 5 is sufficient, we know that every parent/guardian pg can perform the operation “file” on objects that they own with the type “ComplaintRecord.” For all the objects that parent/guardian pg owns, owner_objects(s) where $0 \leq |\text{owner\_objects(s)}| \leq n$ and $n \geq 1$, if none of the object types is “ComplaintRecord,” the parent/guardian pg does not have the permission to file a complaint. If the object type is “ComplaintRecord,” then parent/guardian pg has the permission to file a complaint. When the parent/guardian pg successfully files a complaint record, this event e will be logged and stored in the system. If the object owner (parent/guardian pg), has set up an acknowledgement channel c, an acknowledgement of the event e will be sent via c.

4.4.6 Constraint 6: The right to find out where private information has been shared for purposes other than a game

In order to describe constraint 6, we first introduce a preliminary constraint 6a, which states that recipients must be specified if the purpose of access is other than for a game.

Preliminary Constraint 6a: Recipients must be specified if the purpose of access is other than for a game. Description: for any subject *s* (1) performs a "read" operation op on an object *o* (2) for a purpose PP other than "game" (a) then the recipients must not be empty or access is denied.

$\forall$ s $\in$ SUBJECTS, pg $\in$ PARENTS, u $\in$ USERS, op $\in$ OPS, o $\in$ OBJECTS, PP $\subseteq$ PURPOSES,

u $\in$ subject_user(s)

$\wedge$ op = ("read"), (1)

$\wedge$ PP $\cap$ {"Game"} = $\emptyset$ (2)

$\Rightarrow$

(RP $\neq \emptyset$, privacy_access(s, u, op, o, PP, RP) = (_, _, _))

$\vee$ (RP = $\emptyset$, privacy_access(s, u, op, o, PP, RP) = (deny, $\emptyset$, $\emptyset$)) (a)

Proof: Preliminary constraint 6a is necessary because in order for a parent/guardian to find out where his/her child's private information has been shared, it is essential to distinguish the access purposes and result recipients. Thus, if a "read" operation is requested by a subject who is not the user or owner of the location data, the recipients in the request message should not be an empty set when the purpose is other than for the game. Otherwise, access is denied. This can guarantee the access log could record to whom the information has been shared corresponding to the access request. Therefore Constraint 6a is necessary according to the implication of our privacy constraint 6, a parent has

the right to find out where the location of their child has been shared for the purpose other than the game.

Description: the privacy access is (a) allowed, (b) acknowledged, and (c) logged, if and only if (1) a parent *pg* (2) performs a "findDisclosure" operation on his/her own child's object *o* (3) which is a type of "anyLocationObjectType."

$\forall$ s $\in$ SUBJECTS, pg $\in$ PARENTS, u $\in$ USERS, op_1, op_2 $\in$ OPS, o $\in$ OBJECTS, PP $\subseteq$ PURPOSES, RP $\subseteq$ Recipients, t_1, $t_2 \in$ TIMESTAMP,

(PP $\cap$ {"Game"} = $\emptyset \Rightarrow$ RP $\neq \emptyset$) (Preliminary Constraint 6a)

pg $\in$ user_parent(u) $\wedge$ u $\in$ object_user(o) $\Rightarrow$ pg $\in$ object_owner(o)

$\wedge$ op_1 = "findDisclosure" $\wedge$ op_2 = "read" (1)

$\wedge$ o $\in$ owner_objects(pg) $\wedge$ type(o) = "anyLocationObjectType" (2)

$\forall$ (pg, op_2, o, PP, RP, _, _, _, t_2) $\in$ ACCESS_LOGS where $t_1 \geq t_2$

$\Rightarrow$

$\exists$ c $\in$ COMMUNICATION_CHANNELS, e $\in$ EVENTS,

privacy_access(pg, op_1, o, _, _) = (permit, _, _), (a)

e = (pg, op_1, o, _, _, permit, _, _, t_1), c = com_channel(object_owner(o)),

acknowledgement(object_owner(o), c, e), (b)

log(e) (c)

Proof: the proof consists of two parts: i) showing Constraint 6 is necessary, and ii) showing Constraint 6 is sufficient.

Constraint 6 is necessary according to our privacy constraint 6 that a parent/guardian has the right to find out where the private information of their child has been shared for the purpose other than the game. Therefore, privacy access is allowed, acknowledged,

and logged if a parent/guardian pg requests to find out where their own child's location record object o has been shared for the purpose(s) other than the game.

To show that constraint 6 is sufficient, we first make use of the Preliminary Constraint 6a. From Preliminary Constraint 6a, we know that for any request on performing the "read" operation on object o, which the requester is not the owner of the object, with the purpose other than the "game," the recipients must be specified. With a set of events in the system to record any "read" operation request, we can find out who has disclosed the private records to which recipients. Therefore, the object owner pg is allowed to perform a "findDisclosure" operation to find out how their child's location records are shared other than for the purpose of the game. This operation returns all the events in the systems where any subject performs a "read" operation on object o, with purposes other than "game," and includes the recipients, access decision, obligations, retention, and time.

Before the subject pg performs a "findDisclosure" operation on object o at the time t_1, the access logs may have contained a set of events that a subject s performed an op2 = "read" operation on object o, where object_owner(o) = pg. If no such event ever occurred, the system will return an empty set to parent/guardian pg. In the case of any event (s, op_2, o, PP, RP, _, _, _, t_2) which exists in the access logs, this means that subject s must have performed a "read" operation on object o if and only if s performed the operation at time t_2, where $t_1 \geq t_2$. Therefore, the system will return the events $\{e \in ACCESS\_LOGS \mid e = (s, op_2, o, PP, RP, \_, \_, \_, t_2) \wedge \text{object\_owner}(o) = pg \wedge t_1 \geq t_2\}$ to the subject if and only if $PP \cap \{\text{"Game"}\} = \emptyset$ and $RP \neq \emptyset$. As a result, parent/guardian pg can find out where his/her child's location data has been shared for purposes other than the game if and only if $\{e \in ACCESS\_LOGS,$ where $e = (s, op_2, o, PP, RP, \_, \_, \_, t_2) \wedge \text{object\_owner}(o) = pg \wedge t_1 \geq t_2\} \neq \emptyset$.

4.5 Algorithm for Access Control Decision with Privacy Enforcement

This section presents an algorithm for access control decisions with privacy enforcement.

4.5.1 Prerequisites

A privacy model proposed by Rezgui et al. [152] has a three-dimensional privacy infrastructure: user privacy, services privacy, and data privacy. Based on this model, the access control model allows parents/guardians to specify their privacy preferences on how the service provider can use, store, and disclose the location information of their children. The privacy access control model interprets privacy data based on a set of restriction rules set up by the parent/guardian. Our model assumes that a child's location data objects are associated with a data privacy profile. In our extended access control model, we provide a primary mechanism to allow parent/guardians to express restrictions for their child's location data objects. We assume that whenever a subject requests access to a location object, the restriction in the privacy rule has a corresponding rule in the data privacy profile.

4.5.2 Privacy Rules

Here is the general privacy rule (based on PIPEDA basic principle and Power et al.):

```
With Parent/guardian's consent,
ALLOW mobile service as part of [Subject]
To perform [Operation] on location data [Object]
Only for legitimate [Purposes] to [Recipients]
And then carry out [Obligations] and [Retentions].
DENY otherwise.
```

The *Subject, Operation,* and *Object* are defined in the core access control model in Section 4.1.1. *Purposes, Recipients, Obligations and Retentions* are the privacy entities defined in Section 4.2.1. The privacy rule can be described as follows:

A subject has access to an object, only if the access is authorized by the core access control. Also, the subject needs to specify the purpose(s) of the access and the recipient(s) of the result of the access operation. The purpose(s) and the recipient(s) must be legitimate according to the access of the object defined by the owner or an authority such as the government. Thus, obligations and a retention policy will be returned as a response message if the access is allowed. The subject must also comply with the obligations and the retention policy. The access request will be denied otherwise.

The privacy access control model will address all of these requirements. In section 4.5.3, we present an access control decision making algorithm for the privacy access control model.

4.5.2.1 Policy Rule Creation

Parents can create policy rules for their child's data through the process illustrated in Figure 4.5. This process is done through a mobile web interface on the device, which will be described more thoroughly in Chapter 5. The policy rule creation process starts with the initialization phase, in which first step is for the parent to configure themselves as the child (user)'s parent/guardian. By mapping a parent/guardian to a child user, the parent/guardian becomes the owner of the child's data. Next, the parent/guardian consents to the End User License Agreement (EULA) on behalf of the child, agreeing to the terms of the mobile service. Lastly, the parent/guardian sets their communication channel (e.g. email address) and preferences for receiving acknowledgements of privacy updates related to their child's data. Next, the parent/guardian can create policy rules according to their preferences for how their child's data can be collected and shared. This model uses positive authorization, in which parents define the rules for what is allowed. To create a policy rule, the parent/guardian first specifies the subject (their child), the object (e.g. absolute location data), the allowed operation (e.g. read), the allowed purposes (e.g. game purpose), and the allowed recipients (e.g. other users in-game). Next, the parent/guardian specifies the obligations and retention policies that

the recipient must comply to in order to receive the data object. After this rule is created, the Step 2 process can be repeated to create as many rules as desired.

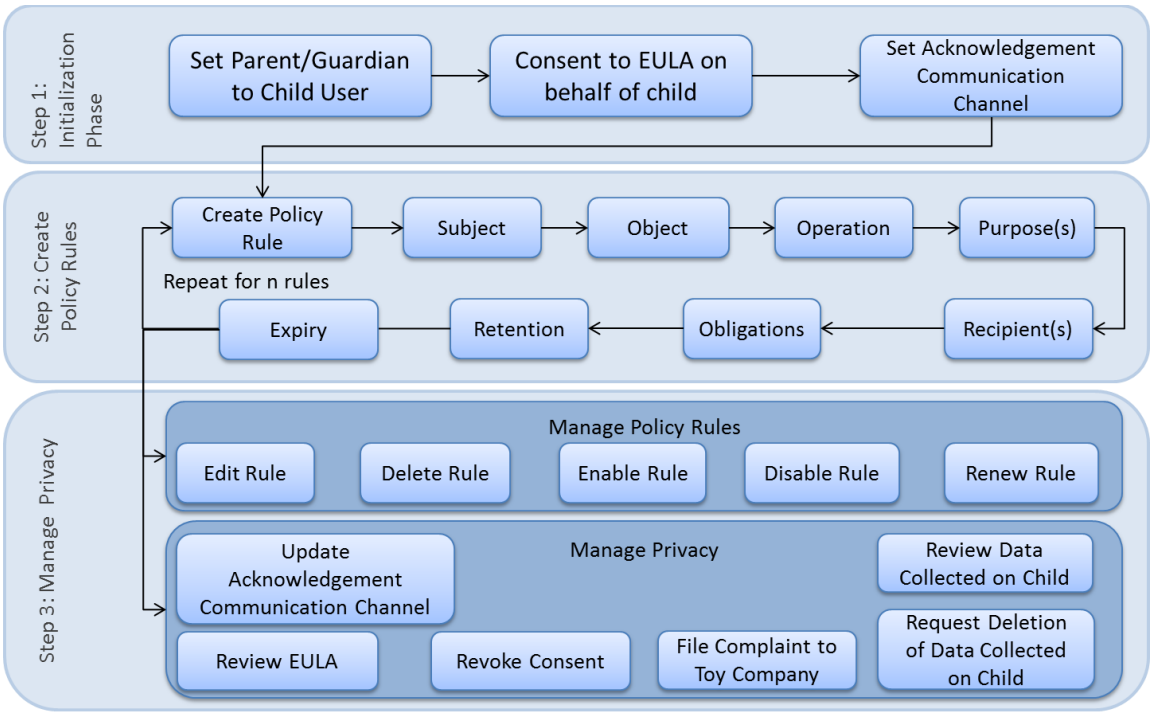

Figure 4.5 Policy Rule Creation Process

4.5.3 Algorithm for Access Control Decisions with Privacy Enforcement

The access control decision algorithm in the privacy access control model is illustrated as follows:

```
While(true){
      //Step 1: Get access requests from the subject
      If request (SUBJECTS s, USERS u, OBJECTS o, OPS op, PURPOSES {pp1,
      …, ppn}, RECIPIENTS {rp1, …, rpm}){

      //Step 2: Process the Request

            //Step 2.1: Check object user and ownership
            USERS u = object_user(o)
            OWNERS owr = object_owner(o)

            //Step 2.2 Retrieve corresponding privacy rules
            PRIVACY_RULES rule = get_privacy_rules(s, u, op, o,
            {pp1,…,ppn}, {rp1,…,rpm})

            //Step 2.3 Check acknowledgement communication channel
            COMMUNICATION_CHANNELS c = com_channel(owr)
```

```
      //Step 3: Make decision
      DECISIONS d = deny

            //Step 3.1 Check permission from core access control model
            PRMS p = assigned_permission(s)

            //Step 3.2 Check legitimate purposes
            if ( p ∧ rule.pp = {pp1, …, ppn}){

                  //Step 3.3 Check legitimate recipients
                  if(rule.rp = {rp1, …, rpm}){

                        //Step 3.4 Final decision
                        d = rule.decisions
                        OBLIGATIONS {obl1,…,oblp} = rule.obligations
                        RETENTIONS rt = rule.retentions
                  }
            }

      //Step 4: Return response and acknowledgement
      if(d = permit){

            //Step 4.1 Return allow, obligations, retention policy
            response(d, {obl1,…,oblp},rt)

            //Step 4.2 Send acknowledgement (if applicable)
            EVENTS e = (s, u, op, o, {pp1,…,ppn}, {rp1,…,rpm}, d,
            {obl1,…,oblp}, rt, time)
            Acknowledgement ack = Acknowledgement(owr, c, e)
      }
      Else{

            //Step 4.1 Return deny, null, null
            response(d, null, null)

            //Step 4.2 Send acknowledgement (if applicable)
            EVENTS e = (s, u, op, o, {pp1,…,ppn}, {rp1,…,rpm}, d, null,
            null, time)
            Acknowledgement ack = Acknowledgement(owr, c, e)
      }

      //Step 5: Write audit trail (log files) for the above steps
      log(e)
      }
}
```

The access control decision process is illustrated in Figure 4.6.

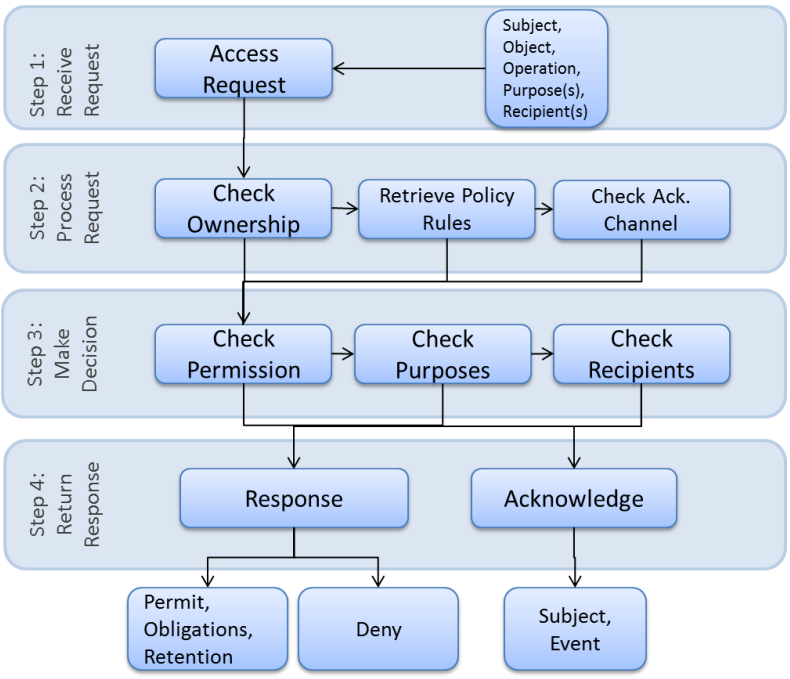

Figure 4.6 Access Control Decision Process

In this mode, a subject first requests access to a user's location information, specifying the subject, object, operation, purpose(s), and recipient(s). After receiving the request, the privacy access control model processes the request as follows: (1) checks the owner of the requested object, then (2) retrieves the corresponding privacy rules from the system, and (3) checks the acknowledgment communication channel for the subject owner. Next, the decision is made by (1) checking the permissions from the core access control model, (2) checking the allowed purposes and then (3) checking allowed recipients. The final decision is made and the system returns a response and acknowledgement. The response can be either permit, along with the obligations and retention policy, or deny. If applicable, the acknowledgement is sent to the subject owner through the predefined acknowledgement channel, and contains the subject and event. Lastly, the model records all of the above in the audit logs.

4.6 Example Scenarios

Referring to a toy computing scenario, in this section we present some example scenarios using Tek Recon, Sphero, and ToyMail (see Chapter 2) to illustrate some possible privacy access control rules.

4.6.1 Scenario 1

Scenario 1: A parent may access his child's location records collected by Sphero. He may update his contact information for receiving acknowledgements. This scenario is illustrated in

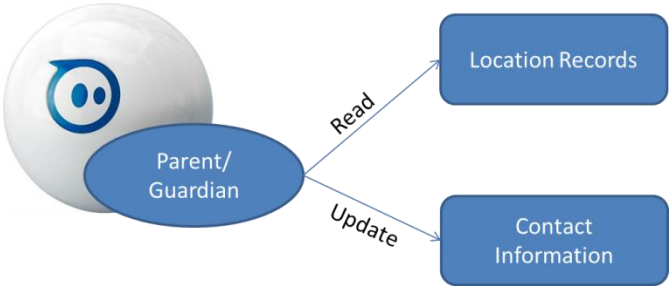

Figure 4.7 Example Scenario 1: Sphero

Privacy rules:

S1.1: A parent/guardian (data owner) is allowed to read or copy his child's location record

```
(Parent/Guaridan, read, locationRecord, _, _, permit, _, _)
(Parent/Guardian, copy, locationRecord, _, _, permit, _, _)
```

S1.2: A parent is allowed to update his/her contact information

```
(owner, update, ContactInformation, _, _, permit, _, _)
```

4.6.2 Scenario 2

Scenario 2: As shown in Figure 4.8, a child using Tek Recon has been connected to a mobile service using location services in a toy computing environment to share his location to his friends and see their locations in return. Once the service receives the user's location record, the service may read and disclose the location information to

other players for the purpose of the game, and delete the records immediately after the game is complete.

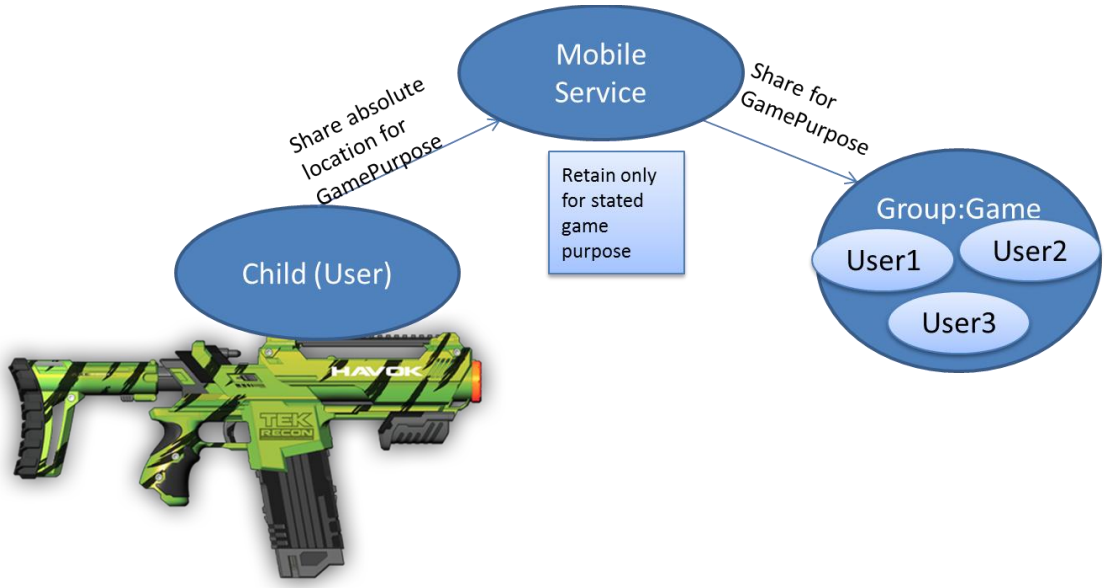

Figure 4.8 Example Scenario 3: Tek Recon

Privacy rules:

S2.1. A service is allowed to read the absolute location record of a user for the purpose of a game if and only if the service follows obligations of disclosure to Group:Game and not to keep the record after stated game purpose has ended.

```
(MobileService, read, Absolute_Location, GamePurpose, Group:Game,
permit, _, StatedPurpose)
```

4.6.3 Scenario 3

As shown in Figure 4.9, the user's contact information and location record may be sent to a business-associated company. The company may share the data with a third party (staff in the research centre).

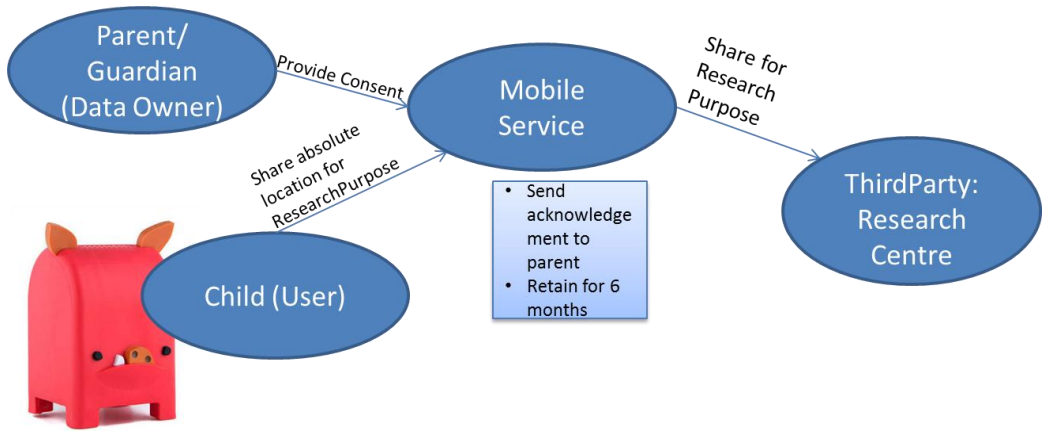

Figure 4.9 Example Scenario 3: ToyMail

Privacy Rules:

S3.1 A child is using location services through a mobile service connected to a ToyMail toy. A service may be allowed to read a user's absolute location for research purposes if and only if the company follows the obligations: the parent/guardian (data owner) provided consent for that usage, and the data must be deleted within a period of 6 months.

```
(MobileService, Read, Absolute_Location_Coarse, ResearchPurpose, Third-
party:ResearchCentre, _, {consent-owner, acknowledge-owner}, legal-
requirement-6months)
```

Note that by default these privacy rules have not been established without the explicit consent of the location information owner. Therefore the system enforces a "deny" decision by default, until the system receives consent from the data owner, at which time the decision attribute will be updated as "allow."

4.7 Summary

This chapter presented a privacy access control model for toy computing with a concentration on location privacy. The model allows parent/guardians to create privacy rules and receive acknowledgements regarding their child's privacy sensitive location data. We defined the rules for the six privacy constraints defined in in Chapter 3, based on privacy requirements for toy computing based on PIPEDA and the 10 privacy principles, and proved how they are sufficient and necessary. Next, we presented the

algorithm for access control decisions for privacy enforcement, and finally we illustrated the applicability of the privacy rules in a practical environment using example scenarios with popular toy computing toys in the industry.

Chapter 5 Proposed Framework and Prototype

In this chapter we present a policy specification language using DPWS, WS-Policy and an extended XACML vocabulary for location privacy. We also provide a technical framework for implementation of the privacy access control model discussed in Chapter 4 using Web and mobile services technologies. This framework is designed to enforce the location privacy preferences defined by parent/guardians for their children who are interacting in a toy computing environment. Finally, we provide a prototype implementation of this framework and a mockup interface for configuring privacy preferences.

5.1 Scope and Prerequisites

5.1.1 Scope

This model is built from the perspective of privacy when a service is requesting access to end device location resources. In this model, depicted in Figure 5.1, the end user's device is acting in the role of resource provider and the Web service is in the role of the requestor. There is a third entity, the Walled Garden Module (WGM), which acts as a trusted module to make access decisions for the mobile device. This will be discussed in greater detail later in the chapter. The model works on a per session basis, rather than per request. This end-to-end session between the three devices takes place upon the initial connection when the service is requesting location information form the user in order to provide services.

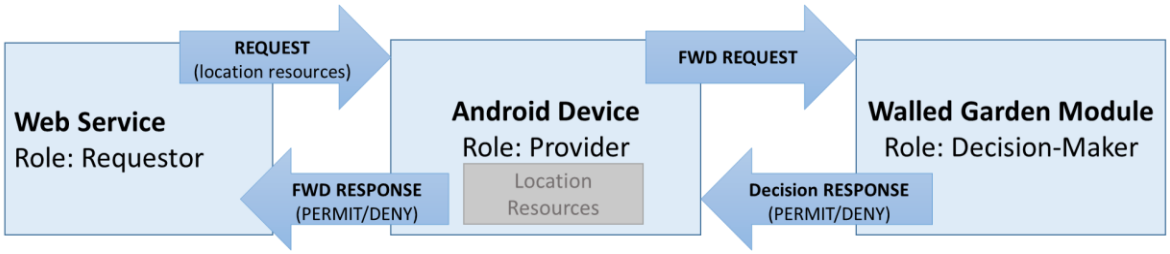

Figure 5.1 Request/Response Session Model

The request is made by the service provider for the user to provide their absolute location (latitude and longitude). Once this location information is collected, the service may share the location with other entities (as outlined in their privacy policy). Sharing this information from the service to a third party will involve a different framework for communication, which is beyond the scope of this thesis, and is a potential area for future work.

5.1.2 Prerequisites

Entities should be authenticated before the process begins. When a user is engaged in a toy computing system, a function binds the user to the device and mobile service, which is then referred to as the subject. Further, this model assumes that the mobile service has published its privacy policy, which must be accurate and comply. Also, the parent/guardian must have published their privacy preferences onto the web server.

5.2 Technical Framework for Privacy Enforcement

This section presents the technical framework for privacy enforcement based on the IETF Abstract Model for Policy Enforcement [103]. First we will explain the entities involved, which will then be presented an illustrated model of the framework which describes how they interact with each other to facilitate access requests and decisions for privacy enforcement.

5.2.1 Description of Entities

5.2.1.1 Mobile Service (Requestor)

In this model, the service is acting in the role of the requestor. The requestor is attempting to access resources from the mobile device in order to provide appropriate services. A mobile service maintains a privacy policy as described below:

- ***Privacy Policy****:* The mobile service has its own privacy policy which outlines information including how it will collect, manage, share, and retain the user's personal data. The privacy policy is provided in XACML. We will go into further detail about privacy policies and vocabulary in a later section.

5.2.1.2 Mobile Device (Provider)

The mobile device acts as the provider in order to provide resources to the mobile service. Typically a mobile device will be owned by a single user. The mobile device hosts the following:

- ***Resources****:* Resources located on the device are the object that the requester is attempting to gain access to. While this is privacy focused framework, this can include any type of resource that will provide personal and/or context-based information. For the purpose of this thesis, we will concentrate on location resources. Location resources provide data such as the user's GPS coordinates and/or altitude, in an event or trace, as defined earlier in this chapter.
- ***End Point Device Profile (EPDP)****:* As part of DPWS, an EPDP exists to identify each device on the network [153]. The EPDP is based on DPWS, which allows for the implementation of mobile devices and services that combine several devices such as SOA.
- ***Policy Enforcement Point (PDP)****:* Each device has its own Policy Enforcement Point, proprietary to each device, which enforces the access decisions received from the PDP. The PEP will permit or deny the access requests based on the decision.

5.2.1.3 Walled Garden Module (Decision-Maker)

The Walled Garden Module (WGM), as introduced in Chapter 1, acts as the decision maker in this scenario. The WGM can be located either as a protected module on the end user's device, or on an external device such as a server. The WGM contains the following items:

- ***User Privacy Preferences (UPP)****:* These preferences are predefined by the user, associated with their EPDP and stored on the WGM. The UPP allows the user to define their preferences for how and which of their data will be collected, shared, retained, etc. These preferences will be defined in P3P with an extended vocabulary for location data, which will be described in more detail later in this chapter.
- ***Policy Decision Point (PDP)****:* The PDP is the entity that makes access decisions with WS-Policy based on the user's privacy preferences and how they compare to the mobile service's privacy policy. The PDP will compare both policies and send the decision response (PERMIT or DENY) to the PEP for enforcement.
- ***Authorization Database (AD):*** The authorization database contains the profiles for users, devices, and services, along with corresponding permissions. This model will use positive authorization based on the contents of the authorization database, which defines a whitelist of what is permitted. The authorization database contains a pool of accepted entities, including accepted users, mobile services, and mobile devices.

5.2.2 Technical Framework Model

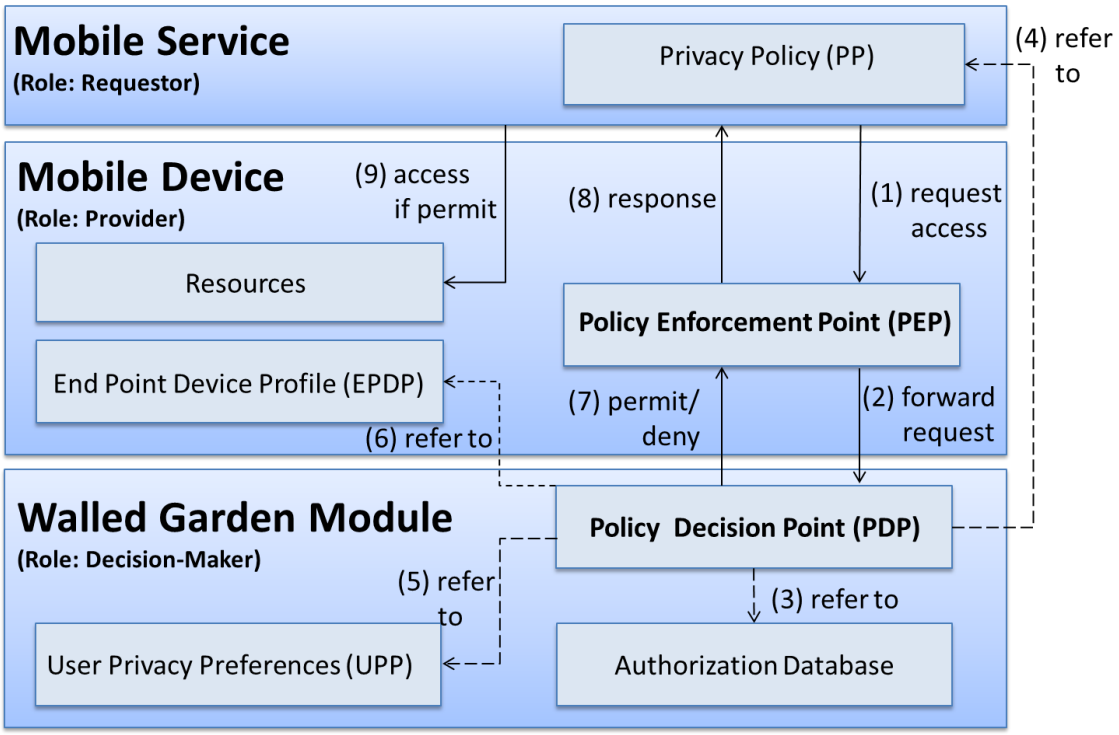

Figure 5.2 Technical Framework Model

Our formal model for privacy enforcement is illustrated in Figure 5.2. In this Service Oriented Architecture (SOA) model, the *Web Service* is acting in the role of *Requestor* for resources provided by the mobile device. The *Walled Garden Module* acts as a decision maker for access control, hosting the Policy Decision Point (PDP), which provides the access decision to the Policy Enforcement Point (PEP) for enforcement, as outlined in the IETF Abstract Model for Policy Enforcement [103], in WS-Policy. When the service requires access to a resource on the mobile device, it will (1) send an XML request to the PEP, which will then (2) forward the request to the PDP to make the access decision. The decision process for access control requires the PDP to compare the policies in (3) the authorization database, (4) the service Privacy Policy (PP), the (5) User Privacy Preferences (UPP) in P3P, and (6) the DPWS End Point Device Profile (EPDP). The service's privacy policy outlines how the service will collect, use, retain, and share data collected from the resource. The user's privacy preferences are provided by the user to define how they will allow their data to be collected, used, retained, shared, etc. The

PDP will find the relevant entries in the Privacy Policy and User Privacy Preferences, and then compare them to ensure that the PP is compliant to the user's preferences. The DPWS End Point Device Profile is included in the request to the PDP, which identifies the mobile device to the WGM and associates it with the user's privacy preferences. (7) If the service's policies comply with the user's privacy preferences, the PDP will send a RESPONSE PERMIT granting permission to the resource. If the policies do not comply, it will DENY access. (8) The PEP then forwards the decision RESPONSE to the service, and enforces the decision by either ending the session or (9) allowing the service to connect to location resources.

5.2.3 Mathematical Model for Algorithm

This section will examine the different parts of the model and how it works to protect privacy. The algorithm for the privacy enforcing model is described as follows. In Step 1, the mobile service sends the request to the PEP located on the device. The request contains the subject, user, operation, object, purpose(s), and recipient(s), as described in Section 4.2. Upon receiving a request, the Policy Decision Point will review the Authorization Database, which contains the profiles for users, devices, and services, along with their corresponding permissions. This model will use positive authorization based on the contents of the authorization database, which defines a whitelist of what is permitted. The authorization database contains a pool of accepted entities, including accepted mobile service URI's, and mobile devices. In comparing the policies, the system uses the Access control algorithm presented in Section 4.5.3. After the authorization database, the next step is to compare the user privacy preferences with the service's privacy policy. In this section we define how access decisions are made by the Policy Decision Point (PDP). The strategy which the PDP takes is to compare the access request with the User Privacy Preferences provided by the user, and with the Privacy Policy provided by the Mobile Service. Finally, when the access decision is made by the PDP, the decision is forwarded to the mobile device for enforcement. If permitted, the mobile service binds to the location resource, if denied, the connection is declined. The algorithm is described below:

Pre-requisites: First, as a prerequisite, we check that all of the entities are authorized in the system. When the user is engaged with a toy computing system the subject is formed by binding the user u_g, with the device d_j and a mobile service ms_m. The device also connects to the walled garden module.

$ms_m.uri_i \in$ URI, where URI is the pool of accepted mobile service URI's

$\wedge\ d_j \in$ DEVICES, where DEVICES is the pool of accepted devices

$\wedge\ u_k \in$ owner(d_j), the user(u_k) is the owner of the device d_j

$\wedge\ uri_i \in d_j$(Permit), the requesting URI (uri_i) is in device d_j's pool of accepted URI's

IF $uri_i \notin d_j$(Permit) $\wedge\ uri_i \notin d_j$(Reject)

$s = bind(u_g, d_j, ms_m,) \wedge connect(d_j, wgm_z)$, where $s \in$ SUBJECTS $\wedge\ u_g \in$ USERS $\wedge\ ms_m \in$ MOBILE_SERVICES $\wedge\ d_j \in$ DEVICES $\wedge\ wgm_z \in$ WGM

Policy Enforcement Algorithm:

1. send(ms_m, d_j.PEP, Request(s, u, op, o, pp, rp)), where s ∈ SUBJECTS, u ∈ USERS, op = {"read"}, pp ⊆ PURPOSES, rp ⊆ RECIPIENTS
2. forward(d_j.PEP, wgm_z.PDP, Request(s, u, op, o, pp, rp))
3. checkPolicy(wgm_z.PDP, Request(s, u, op, o, pp, rp)){
   compare Request(s, u, op, o, pp, rp), wgm_k.authDatabase
   if != deny{
   compare(Request(s, u, op, o, pp, rp), ms_m.PP)
   compare(Request(s, u, op, o, pp, rp), wgm_k.UPP)
   compare(ms_m.PP, wgm_k.UPP)
   compare(wgm. , d_j.EPDP)
   if true, return PERMIT;
   else return DENY; }
4. response(wgm_k.PDP,d_j.PEP, response(decision)), where decision ∈ {"permit" | "deny"}
5. forward(d_j.PEP, ms_m, response(decision))

6. if response(decision) == “permit”{

bind(d_j.resource, ms_m)

}

In the current version of this model, we are assuming that policies don’t change. The authorization database contains logs for authorization decisions based on historical accesses. While this makes the system faster because it does not have to review the policies every time, the limitations are that the access decisions may not be up to date if a user has changed their privacy preferences, or if a mobile service has changed its privacy policy. Future works will include version checking to keep the best of both worlds, speeding up access decisions when policies have not changed, but allowing for policies to be kept up to date.

5.3 Policy Language Vocabulary and Functions

In this section we will extend the XACML policy vocabulary for managing access requests to location data. This thesis presents an extension to the XACML vocabulary to include references specific to location data, based on the core and extended access control entities described in Chapter 4.

Table 5.1 Implementation of Access Control Entities in XACML

Core Access Control Entities	**XACML Implementation**
Users	Subjects
Subjects (mobile service)	Subjects
Objects	Resources
Operations	Actions
Permissions	PolicySet

Table 5.2 Implementation of extended privacy entities in XACML

Extended Access Control Entities	**XACML Implementation**
Purposes	<Resource:Purpose> <Action:Purpose>
Recipients	<Subjects>
Obligations	<Obligations>
Retentions	<Retentions>

Table 5.3 Location Resource Attributes

Location Resource Attributes	**XACML Implementation**
Absolute Location (Coarse)	Absolute_location_coarse
Absolute Location (Fine)	Absolute_location_fine
Relative Location	Relative_location

Based on the extended XACML vocabulary for privacy access control for location data, an XACML implementation of a policy, request, and response are illustrated below.

5.3.1 Policy

We have created an example policy, which has been split into two documents: the core XACML policy, and the extended XACML policy with privacy entities. The core XACML policy includes all of the entities for Combined, the below example of a policy can be summarized as follows: MobileToyService can access Bob's coarse absolute location for the purpose of the game, to recipients of the group playing the game. A permitted request must follow the obligation of no disclosure, and no retention.

5.3.1.1 Core XACML Policy

The core XACML policy is defined as follows: subject MobileToyService can perform the action “read” on Bob’s coarse absolute location.

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<Policy

    xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'

    xmlns='urn:oasis:names:tc:xacml:2.0:policy:schema:os' xmlns:xacml-
context='urn:oasis:names:tc:xacml:2.0:context:schema:os'

    xsi:schemaLocation='urn:oasis:names:tc:xacml:2.0:policy:schema:os
access_control-xacml-2.0-policy-schema-os.xsd'

    PolicyId="TestPolicy"

    RuleCombiningAlgId="identifier:rule-combining-algorithm:deny-overrides">

    <Description>Example XACML Access Control Policy</Description>

    <Rule RuleId="1" Effect="Permit">

        <Description>

             Rule 1: The subject MobileToyService can read Bob's coarse
             absolute location data.

        </Description>

        <Target>

            <Subjects>

                <Subject>

                    <SubjectMatch>

                        <AttributeValue>

                           MobileToyService

                        </AttributeValue>

                    </SubjectMatch>

                </Subject>

            </Subjects>

            <Resources>

                <Resource>

                    <ResourceMatch>

                        <AttributeValue>

                           Bob:Absolute_Location_Coarse

                        </AttributeValue>

                    </ResourceMatch>
```

```
                </Resource>
            </Resources>
            <Actions>
                <Action>
                    <ActionMatch>
                        <AttributeValue>
                           Read
                        </AttributeValue>
                    </ActionMatch>
                </Action>
            </Actions>
        </Target>
    </Rule>
</Policy>
```

5.3.1.2 Extended XACML Policy with Privacy Entities

This section presents the extended policy containing the extended policy for privacy entities, which is combined with the core XACML policy above.

```
<Policy
    xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
    xmlns='urn:oasis:names:tc:xacml:2.0:policy:extendedschema:os'
xmlns:xacml-
context='urn:oasis:names:tc:xacml:2.0:context:extendedContextSchema:os
extendedContextSchema.xsd'
    xsi:schemaLocation='urn:oasis:names:tc:xacml:2.0:policy:schema:os
extendedPolicySchema.xsd'
    PolicyId="ExtendedPolicy"
    RuleCombiningAlgId="identifier:rule-combining-algorithm:deny-
overrides">
       <Description>
              Example Extended XACML Access Control Policy
       </Description>
    <Rule RuleId="1" Effect="Permit">
```

```
<Description>

     Rule 1: The purpose must be for "GamePurpose" and
     recipients must be limited to the group of users playing
     the game.

</Description>

<Target>

    <Purposes>

        <Purpose>

            <PurposeMatch >

                <AttributeValue>GamePurpose</AttributeValue>

            </PurposeMatch>

        </Purpose>

    </Purposes>

    <Recipients>

        <Recipient>

            <RecipientMatch>

                <AttributeValue>Group:Game</AttributeValue>

            </RecipientMatch>

        </Recipient>

    </Recipients>

</Target>

    <Obligations>

        <Obligation>

            <ObligationMatch>

                <AttributeValue>No-Disclosure</AttributeValue>

            </ObligationMatch>

        </Obligation>

    </Obligations>

    <Retentions>

        <Retention>
```

```
                        <RetentionMatch>
                            <AttributeValue>No-Retention</AttributeValue>
                        </RetentionMatch>
                    </Retention>
                </Retentions>
            </Rule>
        </Policy>
```

5.3.2 Example Scenario 1: Permit

Recall from Chapter 4, a Request is a 5-tuple <*Subject, Operation, Object, Purpose(s), Recipient(s)*>. In this model, a location access request occurs when a service is requesting access to the location resources on a user's device. A subject is <toys, devices, mobile_service>. The name of the mobile service (associated with its URI) is be used to identify the requestor. The object is a coarse absolute location resource. For the purpose of this work, operation will always be read. In the below example, a mobile service is requesting access to a user's location resources. The subject is identified by the name of the service. The resource is described using the extended attribute value absolute_location_coarse, which identifies that the resource is the user's coarse absolute location. Next, the action is read, and the purpose is stated as game purposes. Lastly, the recipient is limited to the group of other players currently active in the game session. Note that the core and extended request are given in the same document.

5.3.2.1 Example Request 1

```
<Request>
    <Subject>
        <Attribute>MobileToyService</Attribute>
    </Subject>
    <Resource>
        <AttributeValue>current_location_absolute_coarse</AttributeValue>
    </Resource>
    <Action>
```

```
            <AttributeValue>read</AttributeValue>
    </Action>
</Request>
<RequestExtended>
    <Purpose>
        <AttributeValue>GamePurpose</AttributeValue>
    </Purpose>
    <Recipient>
        <AttributeValue>Group:Game</AttributeValue>
    </Recipient>
</RequestExtended>
```

5.3.2.2 Example Response 1: Permit

Response is a 3-tuple *<Decision, Obligation(s), Retention>*, where the decision is either permit or deny, obligations are the terms which the service must agree to, and retention is the retention policy for how long the object can be retained. Based on the above policy, the request will be permitted. A successful response will be returned as follows:

As described above, the response contains a decision (permit), along with the obligations of the service to agree to non-disclosure obligations. Next, the response also includes a retention policy to not retain the data.

5.3.2.3 Example Request 2

In this second example request, MobileToyService is requesting Bob's absolute location for game purposes and marketing purposes.

```
<Request>
    <Subject>
        <Attribute>MobileToyService</Attribute>
    </Subject>
    <Resource>
        <AttributeValue>Bob:location_absolute_coarse</AttributeValue>
```

```
    </Resource>
    <Action>
            <AttributeValue>read</AttributeValue>
    </Action>
</Request>
<RequestExtended>
    <Purpose>
        <AttributeValue>GamePurpose</AttributeValue>
        <AttributeValue>MarketingPurpose</AttributeValue>
    </Purpose>
    <Recipient>
        <AttributeValue>Group:Game</AttributeValue>
        <AttributeValue>ThirdParty:Marketing</AttributeValue>
    </Recipient>
</RequestExtended>
```

5.3.2.4 Example Response 2: Deny

Since the above request does not comply with the policy, the request will be denied.

```
<Response>
    <Result>
        <Decision>Deny</Decision>
        <Status>
            <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
        </Status>
</Response>
```

5.3.2.5 Example Request 3

This request contains an unrecognized subject and a typo in the <Purpose> tag.

```
<Request>
    <Subject>
```

```
        <Attribute>OtherService</Attribute>
    </Subject>
    <Resource>
        <AttributeValue>current_location_absolute_coarse</AttributeValue>
    </Resource>
    <Action>
        <AttributeValue>read</AttributeValue>
    </Action>
</Request>
<RequestExtended>
    <Prupose>
        <AttributeValue>GamePurpose</AttributeValue>
    </Prupose>
    <Recipient>
        <AttributeValue>Group:Game</AttributeValue>
    </Recipient>
</RequestExtended>
```

5.3.2.6 Example Response 3: NotApplicable

Because the request included a typo resulting in an unrecognized field, a response of "NotApplicable" will occur.

```
<Response>
    <Result>
        <Decision>NotApplicable</Decision>
        <Status>
            <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:missing-
attribute"/>
        </Status>
    </Result>
```

5.4 Prototype Implementation

We have developed a prototype implementation of the privacy access control model and privacy enforcement framework. This prototype demonstrates how the framework can be implemented in a real world environment to preserve privacy through mobile services technologies.

5.4.1 Proof of Concept: Policy Enforcement Demo

5.4.1.1 System Architecture

Like in the privacy enforcement framework, the system architecture for the prototype implementation consists of three devices: the client acting as the resource requestor, the host acting as the resource provider, and an external server acting as the Walled Garden Module for making policy decisions. In this simulation, the host device is the one that the child would be using during a toy computing game. The client is acting in place of a mobile service which is attempting to access the host's location resources. The devices communicate using Java Multi Edition DPWS Stack (JMEDS) [154], which is a lightweight, modular and extendable software framework for DPWS in Java-based environments including Android.

In this BYOD-like architecture, the Walled Garden Module provides a trusted platform for making access decisions based on the policies. Parents can create and store their privacy preferences for their children on the Walled Garden Module, which will make access decisions for the child's mobile device. This also prevents large amounts of processing and storage of policies from having to take place on the mobile device. The Walled Garden Module is running an XACML engine by Sun Microsystems [155], along with a custom co-engine we built over top of it with extra entities for location privacy model. The XACML engine and co-engine parse the XACML policies and make an access decision accordingly. Figure 5.3 illustrates the implementation model and program flow.

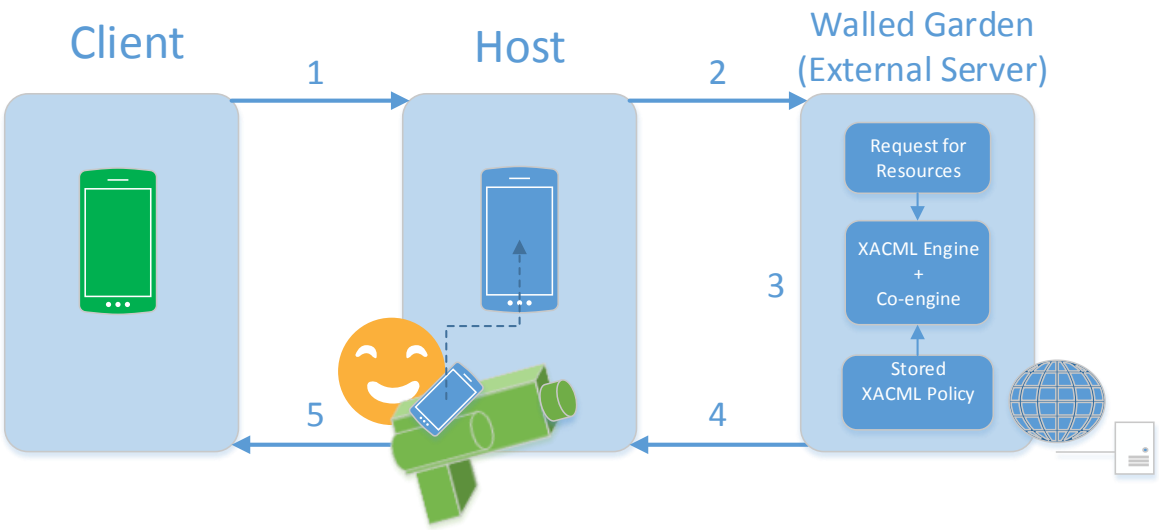

Figure 5.3 Implementation Model

In this model, the process begins when (1) the client device sends a request to the host device via JMEDS using SOAP. (2) The host device will then process this request using XPath sending the noteworthy parts of the message (such as what it is requesting, permissions, and ID of the requestor) to the Walled Garden Module, which is a Linux Server. (3) The Walled Garden Module is running Sun will compare the incoming request with a XACML policy, which can be changed by the system owner and depending on the contents of the request, (4) will issue a "Permit," "Deny," "NotApplicable," or "Indeterminate" decision to the host device, (5) which will act accordingly by either accepting or rejecting the request. Access decisions are described as follows:

- A *permit* decision will permit the requestor to access the requested resources.
- A *deny* decision will not permit the requestor to access the requested resources.
- A decision of *NotApplicable* is a result of a missing attribute, syntax error, or processing error. As a result, the access request will be denied.
- An *Indeterminate* decision means that multiple policies apply to the request and as a result the system is unable to determine a decision. As a result, the access request will be denied.

Referring to our privacy framework in Section 5.2.2, the PDP is the XACML engine and co-engine located on the Walled Garden Module, which makes the policy decisions based on policy rules in the stored policy. The PDP sends the decision to the PEP, which is the host device, to enforce the decision.

5.4.1.2 Technical Configuration

Location management on Android devices is done using the Location Manager system, GPS, Cell-ID and Wi-Fi. Each method offers varying levels of accuracy, and ideally the most accurate solution, GPS, will be used. The system maintains a cached coordinate, which is used unless it is considered as too old. In this case, the system will retrieve a coordinate using Wi-Fi. If this coordinate is inaccurate, the system will retrieve a location using GPS instead. Updates on the user's location can be obtained by assigning the Location Manager to request Location Updates from a Location Listener that pinpoints the user's location using one of the mentioned methods.

The WalledGardenModule uses several external libraries as well as default libraries. For the Server application, XPath and Sun's XACML implementation are used to parse the incoming Request Documents and the stored Policies. The mobile application uses XPath to parse the Response from the server. File transfer between the mobile application and the server is done through a TCP socket to ensure file delivery.

Table 5.4 shows the technical configurations of the three devices used in the prototype implementation environment described above. The client and host are both Android devices, and the server, acting as the Walled Garden Module, is running Ubuntu.

Table 5.4 Technical Configuration

Walled Garden Module (Web Server)	
Manufacturer	IBM
OS	Linux Ubuntu 14.04.1 LTS Server x64
CPU	Intel Xeon E5-2609 v2 @ 2.50GHz
Memory	2GB

Host Device (Service Provider)	
Manufacturer	Huawei
Model	U9510E
OS	Android 4.0.4
CPU	Quad-core Cortex-A9 @ 1.4GHZ
GPU	Vivante GC4000
Memory	1GB
Client Device (Service Requestor)	
Manufacturer	HTC
Model	One V
OS	Android 4.0.3
CPU	Scorpion @ 1.0GHz
GPU	Adreno 205
Memory	512MB

5.4.2 Mockup Interface Demo

We have developed a mockup interface for parents/guardians to use in an initial setup to configure preferences and create policy rules, as described in Section 4.5.2.1. These options would appear during initial setup of a toy computing application.

5.4.2.1 Profile Setup

The first step in the configuration process is the Profile Setup phase. The Profile Setup phase includes three sections, the Parent/Guardian Contact Details, Child Information, and Privacy Policy Review.

shows the first two screens of the Profile Setup Phase. In the first screen, the parent/guardian enters their basic information including name and email address, and then selects if they wish to receive email updates on their child's privacy-related information. Next, on the Child Information page, the child's first name is entered for management purposes, and the parent/guardian then agrees to take ownership over their child's data.

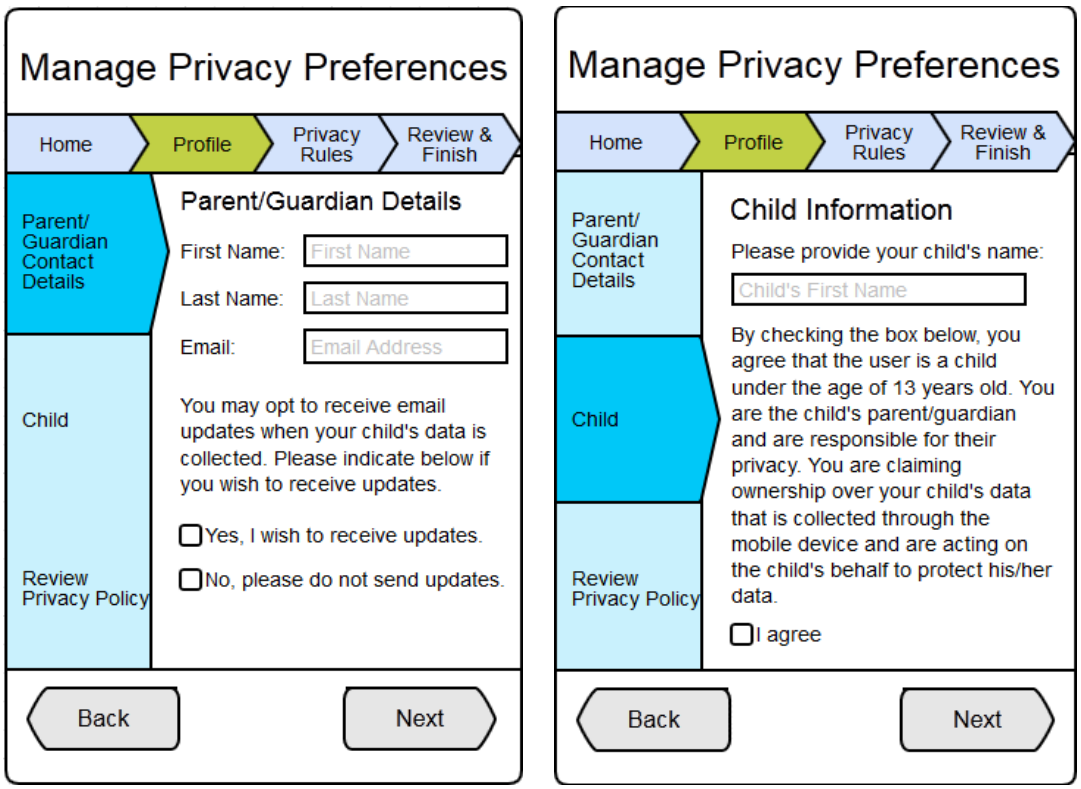

Figure 5.4 Profile Setup: Parent/Guardian Details and Child Information

Next, the privacy policy of the mobile toy application is presented to the parent/guardian to review. The parent/guardian reviews the policy and must confirm that they have read and agree to the terms before proceeding.

Figure 5.5 shows this screen with the *Tek Recon* privacy policy. By agreeing to the terms, the parent/guardian is providing consent on their child's behalf.

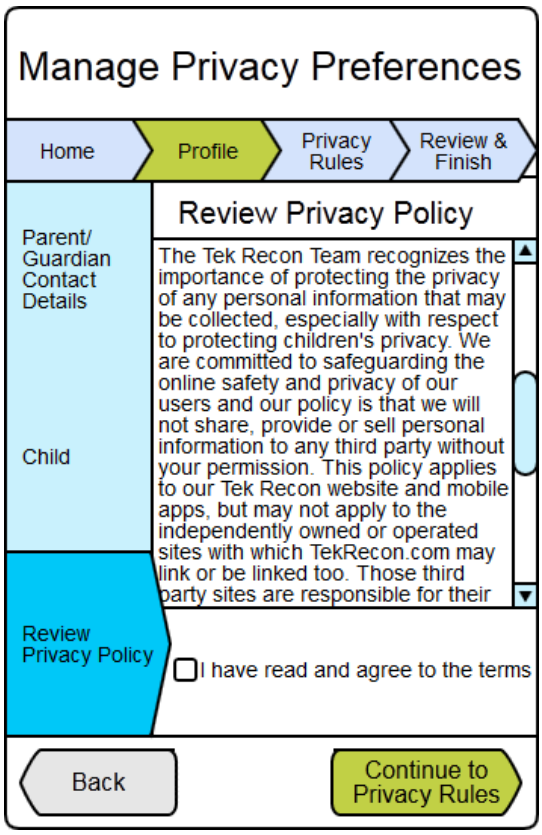

Figure 5.5 Review Privacy Policy

5.4.2.2 Configuring Privacy Rules

The next phase of the setup is the Privacy Rule creation phase. In this phase, the parent/guardian is able to create one or more privacy rules for how their child's private location data is used. By default there are no policy rules yet configured. As shown in Figure 5.6, a new rule can be created or a template can be used. Templates of useful policy rules can be provided to simplify the rule configuration process for parents/guardians. However, in this example we will show how to create an entirely new rule from scratch.

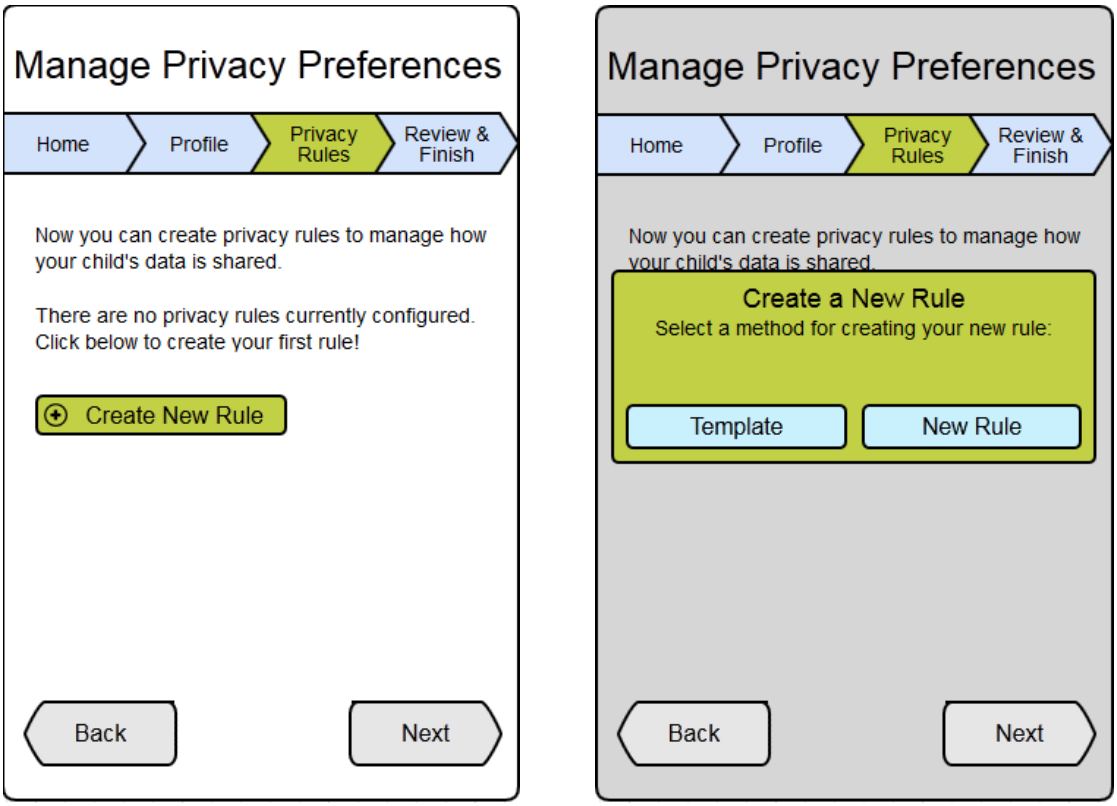

Figure 5.6 Create a New Rule

The first step of creating a new privacy rule is the General Settings, as shown in Figure 5.7. In the General Settings, the parent/guardian can name the rule, provide a description, and set an expiry date for how long the rule will be in effect. Next, in the Core Access Control settings, the mobile service (subject), location resource (object), and operation are selected. The objects selected are the absolute location and relative location.

Next, the settings for Purposes and Recipients are also presented in Figure 5.7. The parent/guardian chooses from a list of purposes they wish to accept, as well as a list of types of recipients. The types of recipients can be expanded to be more specific, such as Third-Party: Marketing, or Group: Game Players.

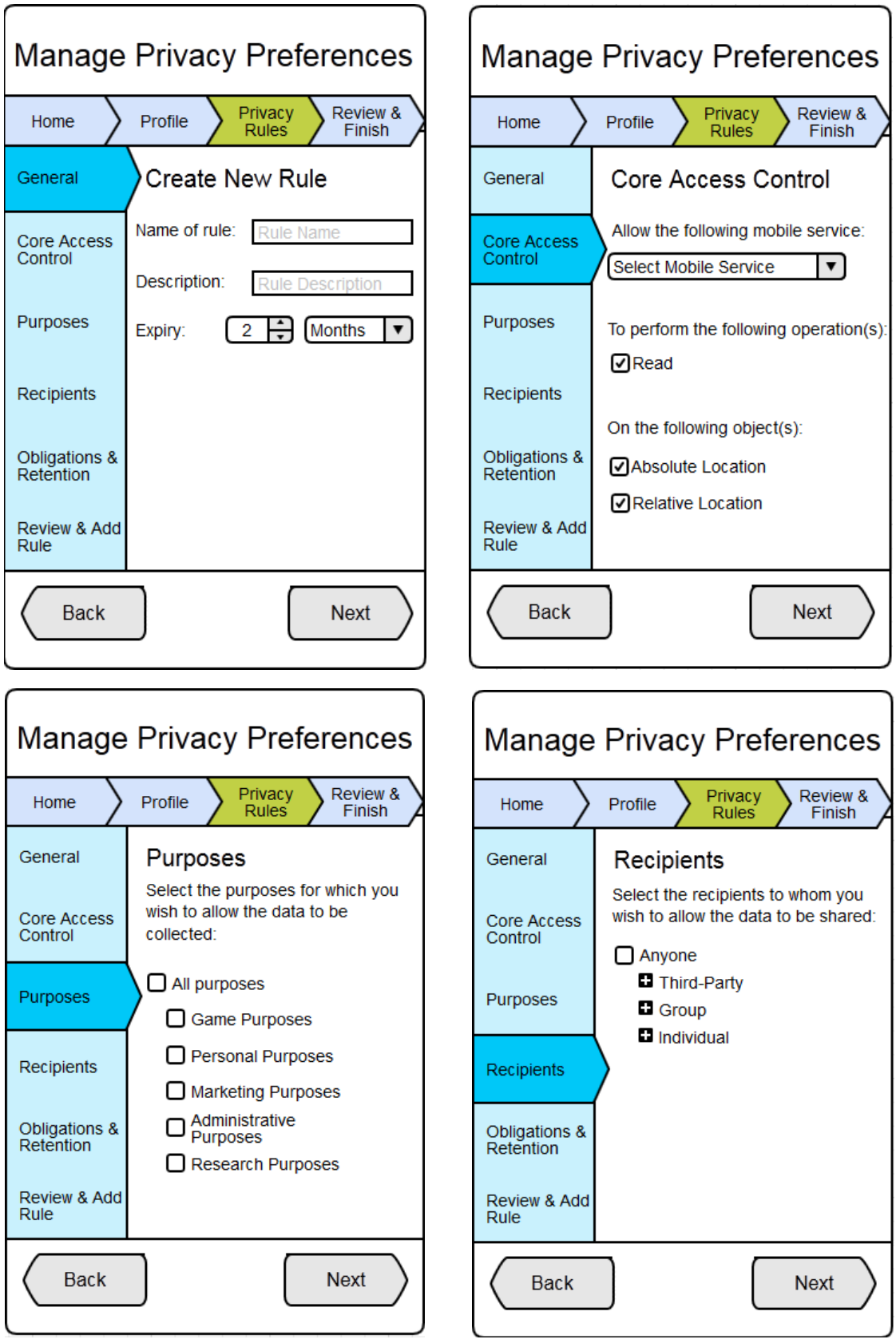

Figure 5.7 Create New Rule: General, Core Access Control, Purposes and Recipients

The next steps are the Obligations and Retention settings, and then finally reviewing and adding the rule, as shown in Figure 5.8. In Obligations and Retention settings, the parent/guardian first selects the obligations that the service must comply with upon receiving the child's data. Obligations can include compliance with PIPEDA or COPPA. The parent/guardian can also search from a list of other obligations, or input a custom obligation policy. For retention, the parent/guardian can select how long they wish to allow their child's data to be retained. Finally, on the Review & Add Rule page, the privacy rule is presented in plain English. Once the parent/guardian reviews the rule, they can select "Confirm and Add Rule" at the bottom of the screen.

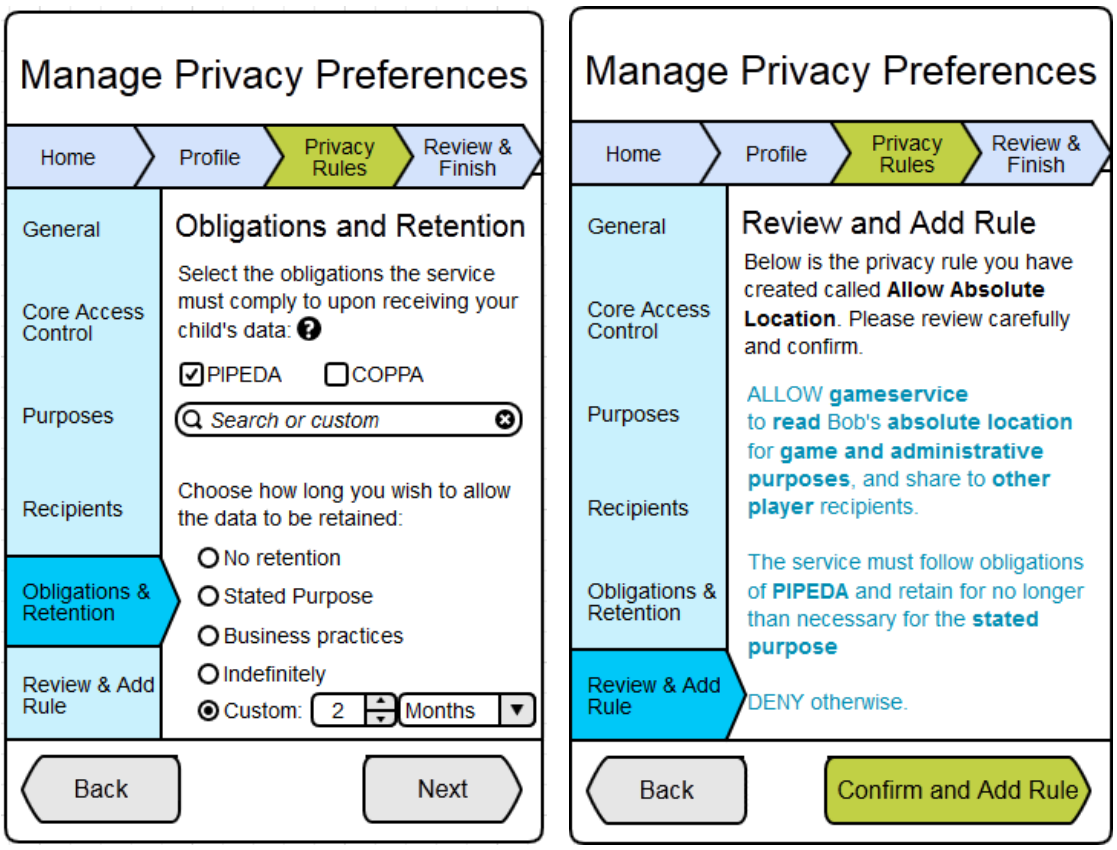

Figure 5.8 Obligations and Retention, and Review and Add Rule

Once a privacy rule is added, the parent/guardian is directed to the Manage Privacy Rules page, illustrated in Figure 5.9. The Manage Privacy Rules page shows a table of all of the configured privacy rules and their status (e.g. enabled, disabled, or expired). This provides options to enable, disable, edit, delete, or create new rules. A parent/guardian can also return to this screen at a later time to manage rules or renew expired rules.

Once the parent/guardian is satisfied with the privacy rules, he/she can select “Next” to be directed to the final Review & Finish page. This page summarizes all of the settings and confirms that the parent/guardian has completed all of the sections. A list of enabled privacy rules and their corresponding expiry dates is also presented. Finally, the parent/guardian can select “Save and Finish” to save their settings and finish the setup. Once the setup is finished, the settings will take effect immediately.

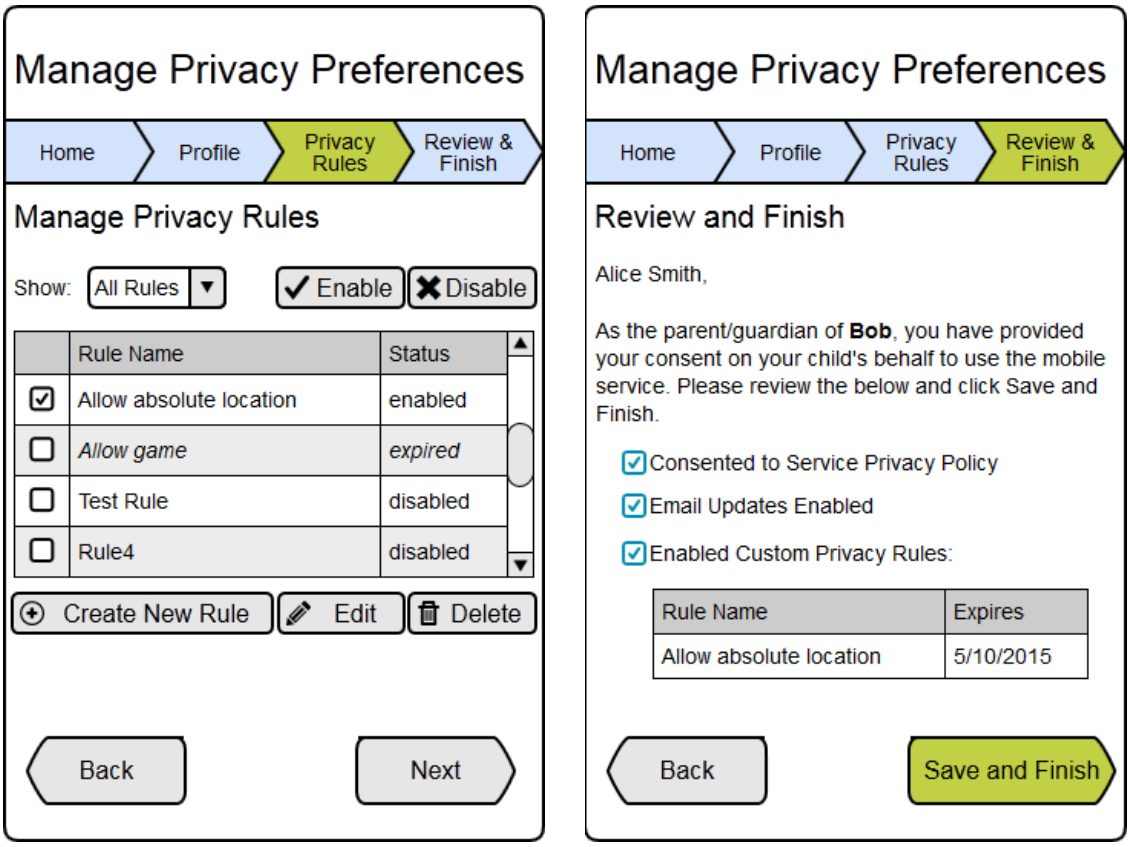

Figure 5.9 Manage Privacy Rules, and Review and Finish

5.5 Summary

In this chapter we presented a technical framework for privacy enforcement based on the IETF abstract model for policy enforcement, and adapted it to a toy computing context using mobile services technologies and the concept of Walled Garden. We showed the mathematical model and algorithm for the framework to explain the policy

decision and enforcement process. Next, we examined the XACML request and response with some examples. Finally, we presented a prototype implementation of the framework model using two Android devices and an Ubuntu server and communicating with JMEDS, as well as a mockup interface for parents/guardians to configure privacy settings.

Chapter 6 **Conclusions and Future Works**

6.1 Thesis Summary

This thesis has aimed to address the unique location privacy requirements for children using toy computing technology. Privacy laws such as PIPEDA and the 10 principles of privacy, as well as the many industry and international organizations such as UNICEF and ITU, stress for the protection of children's personal data online. Motivated by this, we have provided an access control model to protect the location privacy of children in toy computing. While there is no universal privacy framework for toy computing, we have presented a technical policy enforcement framework using a Walled Garden Module. We provided a prototype implementation of this framework using an extended XACML vocabulary. We have presented a privacy access control model designed specifically to protect children's location data in a toy computing environment, allowing parents to create privacy preferences for how their child's location data can be collected, used, shared, and retained.

6.2 Limitations

Although this thesis presents a study of the requirements for privacy based on existing research, legislation and current industry regulations, and validates the requirements through mathematical proofs and proof of concept prototypes. However, there is further work to be done in the form of empirical studies and surveys of toy companies, parents, and children to validate that this model and framework is necessary and meets the requirements of practical application. From an end user perspective, this model requires that parents are able to understand and properly configure the privacy settings to adequately reflect their preferences.

This model and framework relies on a foundation of security. We assume that the mobile device is trusted (TCB). Further, this work operates under the assumption of an

architecture such as Android, where applications are sandboxed. In this architecture, applications require permissions to access resources such as GPS. Another limitation is that service providers must comply with their stated privacy policies, as this model provides limited enforcement in terms of policy compliance.

6.2.1 Further Works for Toy Computing

In the context of toy computing, there are many other types of sensitive context data that can be collected on children, as described in Section 2.1.3.1. The vocabulary presented in this thesis can be extended for other toy computing privacy concerns beyond location. Further, a management interface can be developed for parents/guardians to easily configure the privacy preferences for their children. Future work includes exploring the best way to present the system to parents/guardians so that they can easily set policy options and make informed decisions so that they can be confident about their children's privacy.

6.2.2 Mobile Services Cluster for BYOD

The privacy enforcement framework presented in this thesis can also be extended for a wider range of applications in other areas of pervasive and mobile computing, such as healthcare, transportation systems, manufacturing, infrastructure protection, power grids, and process control [42]. A future area of research is to adapt the privacy framework to a BYOD cluster infrastructure, using the concept of the *Walled Garden Module* built on a Raspberry Pi computer to connect to the mobile devices via USB or Bluetooth as shown in Figure 6.1. In this model, Raspberry Pi computers [156] which consist of a credit-card-sized single-board computer, are used to build a scalable, interoperable, and flexible Mobile Services Cluster in a Lego bricks-built server rack with easy movability and composability. Each system represents a simulated mobile service which is interconnected through a multi-root tree topology in a Top of Rack (ToR) switch manner, in which the computers in the same rack are connected to one or two Ethernet switches installed inside the rack and to the rest of the topology through an OpenFlow enabled aggregation switch. OpenFlow is an open standard that can support

experiments to run on a network, without requiring vendors to expose the internal workings of their network devices such as Ethernet switches, routers and wireless access points.

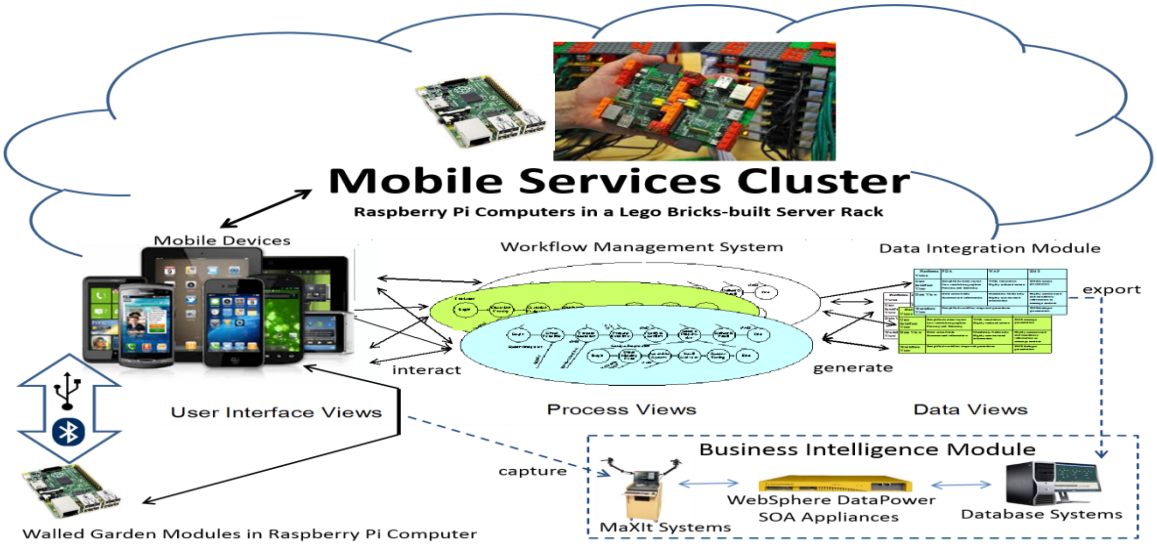

Figure 6.1 Mobile Services Cluster for BYOD

Further, the framework can be extended for security policy enforcement. Figure 6.2 shows the technical model of our proposed framework from the perspective of security policy enforcement, where the mobile device acts in the role of requestor for resources provided by the mobile services. In this case, the goal of the Walled Garden Module is act as a broker to enforce the security policies for the mobile service. The enforcement decision is once again determined by the PDP, this time located on the service side, which compares the service's security policy to the EPDP of the mobile device. If permission is granted, the resources are sent to the *Intermediate Resources Storage* based on the concept of *Isolation Space* [157] within the Walled Garden Module, which can then be accessed by the device. The Walled Garden Module contains data or application processing within a secure framework on the personal device (BYOD) so that it is segregated from personal data.

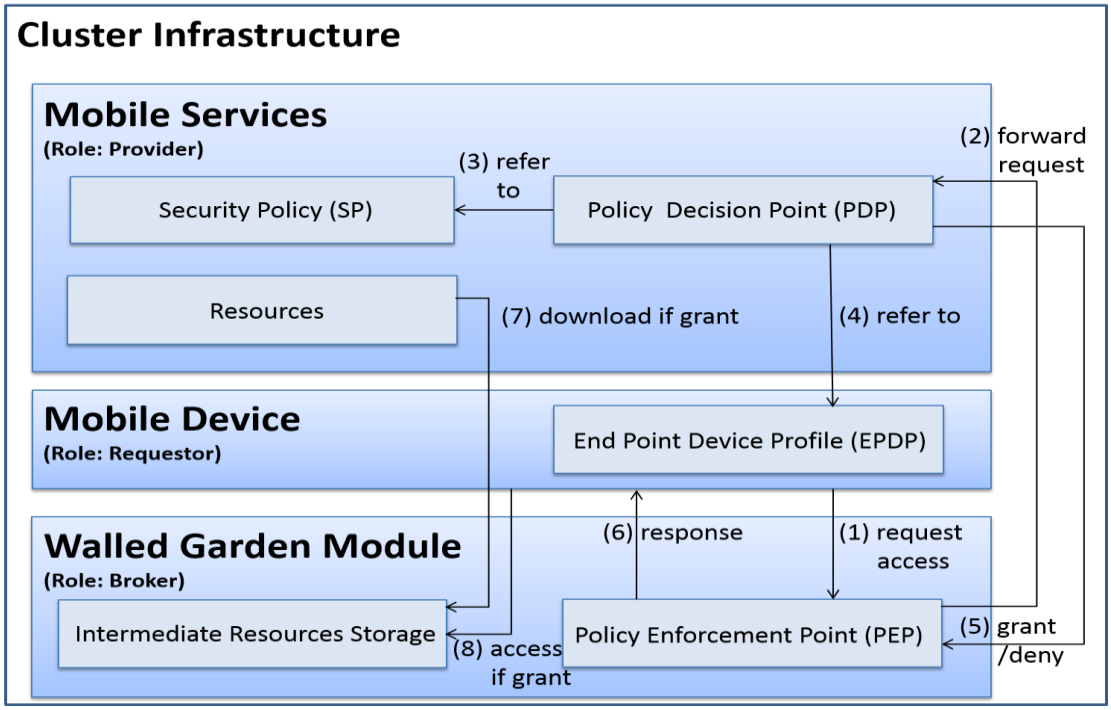

Figure 6.2 Security Policy Framework

6.3 Thesis Conclusions

This thesis has presented a privacy access control model and technical framework for protecting children's location data in a toy computing environment. Toy computing is a developing research area and to the best of our knowledge, this concept of location privacy policy-based access control specific to toys has scarcely been explored in other research works. There is currently no widespread industry model for privacy enforcement for toy computing. This thesis presents a novel access control model and technical framework for children's location data in a toy computing environment, which to the best of our knowledge is the first of its kind.

References

[1] M. LaMonica, "Mobile Apps Reshape Toys and Learning," 18 April 2012. [Online]. Available: http://www.cnet.com/news/mobile-apps-reshape-toys-and-learning/. [Accessed December 2014].

[2] K. T. Bradford, "The Future of Toys Is Augmented Reality," 27 February 2014. [Online]. Available: http://www.alleywatch.com/2014/02/the-future-of-toys-is-augmented-reality/. [Accessed December 2014].

[3] A. Smith, "Tiny Sensors are a Game Changer at Toy Fair 2014," 19 February 2014. [Online]. Available: http://www.huffingtonpost.com/andrea-smith/tiny-sensors-are-a-game-c_b_4814579.html. [Accessed 2014].

[4] W. Greenwald, "Augmented Reality Takes Center Stage at Toy Fair 2012," 14 February 2012. [Online]. Available: http://www.pcmag.com/article2/0,2817,2400230,00.asp. [Accessed 2014 December].

[5] Toy Industry Association, "Toy Trends," Toy Industry Association, 2015. [Online]. Available: http://www.toyassociation.org/TIA/Industry_Facts/trends/IndustryFacts/Trends/Trends.aspx. [Accessed 2015].

[6] The NPD Group, Inc., "2013 Review of the Global Toy Market," Toy Industry Association, 2014.

[7] U. Tansel, "Toys and Games: Global Trends, Developments, and Prospects," Euromonitor International, 2015.

[8 Toy Industry Association Inc., "Economic Impact of the Toy Industry 2013 Summary

] Report," Toy Industry Association Inc., 2012.

[9 Gartner, "Key Challenges in BYOD," 2014. [Online]. Available:
] http://www.gartner.com/technology/topics/byod.jsp. [Accessed September 2014].

[1 P. Beckett, "BYOD - Popular and Problematic," *Network Security,* vol. 2014, no. 9, pp.
0] 7-9, 2014.

[1 OASIS, "eXtensible Access Control Markup Language (XACML) Version 3.0," OASIS,
1] 2013.

[1 Office of the Privacy Commissioner of Canada, "Guidelines for Online Consent," May
2] 2014. [Online]. Available:
https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_e.asp. [Accessed February 2015].

[1 International Telecommunication Union (ITU), United Nations Children's Fund
3] (UNICEF), Guidelines for Industry on Child Online Protection, Geneva, Switzerland: International Telecommunication Union, 2014.

[1 S. Livingstone, L. Haddon, A. Gorzig and K. Olafsson, "Risks and Safety on the
4] Internet: The Perspective of Europan Children, Full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries," London School of Economics and Political Science, London, 2011.

[1 A. Schrock and D. Boyd, "Online Threats to Youth: Solicitation, Harassment, and
5] Problematic Content," Berkman Center for Internet & Society, Harvard University, Cambridge.

[1 U.S. Department of Justice, National Sex Offender Public Website, "Raising awareness
6] about sexual abuse: Facts, myths and statistics," [Online]. Available:
http://www.nsopw.gov/en/Education/FactsMythsStatistics. [Accessed March 2015].

[17] D. Salomon, "Privacy and Trust," in *Elements of Computer Security, Undergraduate Topics in Computer Science*, Springer, 2010, pp. 273-290.

[18] United Nations Children's Fund (UNICEF), "United Nations Convention on the Rights of the Child," United Nations, Geneva, 1989.

[19] Canadian Public Works and Government Services, "Personal Information Protection and Electronic Documents Act," 2000.

[20] Health Canada, "Industry Guide to Health Canada's Safety Requirements for Children's Toys and Related Products," Health Canada, 2012.

[21] I. Reay, S. Dick and J. Miller, "A Large-Scale Empirical Study of P3P Privacy Policies: Stated Actions vs. Legal Obligations," *ACM Transactions on The Web,* vol. 3, no. 2, pp. 6:1-6:34, 2009.

[22] Canadian Standards Association, "Archived - Appendix 3: Model Code for the Protection of Personal Information," 1996. [Online]. Available: http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00076e.html. [Accessed February 2015].

[23] United States Federal Trade Commission, "Children's Online Privacy Protection Act of 1998," 1998. [Online]. Available: http://www.coppa.org/coppa.htm. [Accessed February 2015].

[24] Office of the Privacy Commissioner of Canada, "Policy Position on Online Behavioural Advertising," June 2012. [Online]. Available: https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp. [Accessed November 2014].

[25] Digital Services Advisory Group and Federal Chief Information Officers Council, United States of America, "Bring Your Own Device," 23 August 2012. [Online].

Available: http://www.whitehouse.gov/digitalgov/bring-your-own-device. [Accessed September 2014].

[26] World Economic Forum, "Personal Data: The Emergence of a New Asset Class," World Economic Forum, 2011.

[27] H. D'Hooge and M. Goldstein, "History of the Smart Toy Lab and Intel Play Toys," *Intel Technology Journal,* vol. 2001, no. Q4, 2001.

[28] S. Hinske and M. Langheinrich, "Managing Augmented Toy Environments - A New Perspective for Smart Space Management," in *Proceedings of the 4th International Workshop on Managing Ubiquitous Communications and Services (MUCS)*, Munich, Germany, 2007.

[29] R. Luckin, D. Connolly, L. Plowman and S. Airey, "Children's Interactions with Interactive Toy Technology," *Journal of Computer Assisted Learning,* vol. 19, pp. 165-176, 2003.

[30] L. Plowman and R. Luckin, "Interactivity, Interfaces, and Smart Toys," *Computer,* pp. 98-100, February 2004.

[31] Tech4Kids, "Tek Recon," Tech4Kids, 2013. [Online]. Available: http://www.tekrecon.com/. [Accessed August 2014].

[32] ChineseCUBES, "AR Cubes," 2014. [Online]. Available: https://www.chinesecubes.com/ar_cubes.

[33] V. Woollaston, "Step Aside Ted, There's A New Talking Teddy in Town: WikiBear Connects to the Web to Chat, Answer Questions and Tell Jokes," 20 February 2014. [Online]. Available: http://www.dailymail.co.uk/sciencetech/article-2564015/Step-aside-Ted-theres-new-talking-teddy-town-WikiBear-connects-web-chat-answer-questions-tells-jokes.html.

[3 Sphero, "Sphero," 2014. [Online]. Available: http://www.gosphero.com. [Accessed 4] August 2014].

[3 Toymail Co. LLC, "Toy Mail," Toymail Co. LLC, 2014. [Online]. Available: 5] http://www.toymail.co/.

[3 S. Lee and Y. Y. Doh, "iSpy: RFID-Driven Language Learning Toy Integrating Living 6] Environment," in *CHI '13 Proceedings from the 2013 International Conference on Interaction Design and Children*, Paris, France, 2013.

[3 H. Andreae, P. Andreae, J. Low and D. Brown, "A Study of Auti: A Socially Assistive 7] Robotic Toy," in *IDC '14 Proceedings of the 2014 Conference on Interaction Design and Children*, New York, NY, USA, 2014.

[3 M. D. Gross and M. Eisenberg, "Why Toys Shouldn't Work "Like Magic": Children's 8] Technology and the Values of Construction and Control," in *The First IEEE International Workshop on Digital Game and Intelligent Toy Enhanced Learning (DIGITEL '07)*, Jhongli, Taiwan, 2007.

[3 T. L. Westeyn, G. D. Abowd, T. E. Starner, J. M. Johnson, P. W. Presti and K. A. 9] Weaver, "Monitoring Children's Developmental Progress using Augmented Toys and Activity Recognition," *Personal Ubiquitous Computing,* vol. 2012, no. 16, pp. 169-191, 2012.

[4 S. Hinske, M. Langheinrich and M. Lampe, "Towards Guidelines for Designing 0] Augmented Toy Environments," in *Designing Interactive Systems (DIS) 2008*, Cape Town, South Africa, 2008.

[4 D. Saha, "Pervasive Computing: A Paradigm for the 21st Century," *Computer,* vol. 36, 1] no. 3, pp. 25-31, 2003.

[4 A. Sheth, P. Anantharam and C. Henson, "Physical-Cyber-Social Computing: An Early

2] 21st Century Approach," *Intelligent Systems, IEEE,* vol. 28, no. 1, pp. 78-82, 2013.

[4 Google, "Sensors Overview," developer.android.com, [Online]. Available:
3] http://developer.android.com/guide/topics/sensors/sensors_overview.html. [Accessed September 2014].

[4 Six to Start, "Zombies, Run! 3," Six to Start, [Online]. Available:
4] https://www.zombiesrungame.com/. [Accessed September 2014].

[4 Yelp, "Yelp Mobile," Yelp, 2015. [Online]. Available: http://www.yelp.ca/yelpmobile.
5] [Accessed February 2015].

[4 zomato, "Urbanspoon," zomato, 2015. [Online]. Available:
6] http://www.urbanspoon.com/. [Accessed February 2015].

[4 Instagram, "Instagram," Instagram, 2015. [Online]. Available: http://instagram.com/.
7] [Accessed February 2015].

[4 Facebook, "Facebook Mobile," Facebook, 2015. [Online]. Available:
8] https://www.facebook.com/mobile/. [Accessed February 2015].

[4 Cumulonimbus, "PressureNet," Google Play, 2015. [Online]. Available:
9] https://play.google.com/store/apps/details?id=ca.cumulonimbus.barometernetwork&feature=nav_result#?t=W251bGwsMSwxLDMsImNhLmN1bXVsb25pbWJ1cy5iYXJvbWV0ZXJuZXR3b3JrIl0.. [Accessed February 2015].

[5 A. K. Dey and G. D. Abowd, "Towards a Better Understanding of Context and Context-
0] Awareness," Georgia Institute of Technology, College of Computing, 1999.

[5 B. Schilit, N. Adams and R. Want, "Context-Aware Computing Applications," in *WMCA*
1] *'94*, Washington, DC, USA, 1994.

[5 A. Schmidt, "Interactive Context-Aware Systems Interacting with Ambient

2] Intelligence," in *Ambient Intelligence*, G. Riva, F. Vatalaro, F. Davide and M. Alcaniz, Eds., IOS Press, 2005, pp. 159-178.

[5 R. Dewri, P. Annadata, W. Eltarjaman and R. Thurimella, "Inferring Trip Destinations
3] from Driving Habits Data," in *Workshop on Privacy in the Electronic Society*, Berlin, Germany, 2013.

[5 M. Cherubini, R. de Oliveira, A. Hiltunen and N. Oliver, "Barriers and bridges in the
4] adoption of today's mobile phone contextual services," in *MobileHCI '11*, Stockholm, Sweden, 2011.

[5 MEF, "MEF Global Privacy Report 2013," MEF, 2013.
5]

[5 Futuresight, "User Perspectives on Mobile Privacy - Summary of Research Findings,"
6] GSMA, 2011.

[5 S. Chakraborty, K. R. Raghavan, M. P. Johnson and M. B. Srivastava, "A Framework for
7] Context-Aware Privacy of Sensor Data on Mobile Systems," in *The Fourteenth Workshop on Mobile Computing Systems and Applications (ACM HotMobile2013)*, New York, USA, 2013.

[5 A. Schmidt, M. Beigle and H. W. Gellersen, "There is more to context than location,"
8] *Computer & Graphics Journal,* vol. 23, no. 6, pp. 893-902, 1999.

[5 Merriam-Webster, "Location," [Online]. Available: http://www.merriam-
9] webster.com/dictionary/location. [Accessed January 2015].

[6 National Geographic, "Encyclopedic Entry: Location," [Online]. Available:
0] http://education.nationalgeographic.com/education/encyclopedia/location/?ar_a=1. [Accessed January 2015].

[6 Android, "Location Strategies," Android Developer, 2015. [Online]. Available:

1] http://developer.android.com/guide/topics/location/strategies.html. [Accessed February 2015].

[6 T. Whalen, "Mobile Devices and Location Privacy: Where do we go from Here?," *IEEE*
2] *Security & Privacy,* vol. 9, no. 6, pp. 61-62, 2011.

[6 S. Patil, G. Norcie, A. Kapadia and A. J. Lee, "Reasons, Rewards, Regrets: Privacy
3] Considerations in Location Sharing as an Interactive Practice," in *Symposium on Usable Privacy and Security*, Washington, D.C., 2012.

[6 A. A. Pandit and A. Kumar, "Conceptual Framework and a Critical Review for Privacy
4] Preservation in Context Aware Systems," in *IEEE 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Sanya, China, 2012.

[6 TIME and Qualcomm, "Your Wireless Life: Results of TIME's Mobility Poll," July 2012.
5] [Online]. Available: http://content.time.com/time/interactive/0,31813,2122187,00.html. [Accessed November 2013].

[6 T. Gu, H. K. Pung and D. Q. Zhang, "A Middleware for Building Context-Aware Mobile
6] Services," in *IEEE Vehicular Techology Conference*, 2004.

[6 S. Duri, A. Cole, J. Munson and J. Christensen, "An approach to providing a seamless
7] end-user experience for location-aware applications," *1st International Workshop on Mobile Commerce,* vol. 86, no. 4, p. 20, 2001.

[6 M. Pura, "Linking perceived value and loyalty in location-based mobile services,"
8] *Managing Services Quality,* vol. 15, no. 6, pp. 509-538, 2005.

[6 C. Baber and O. Westmancott, "Social networks and mobile games: the use of
9] bluetooth for a multiplayer card game," in *6th International Conference on Human Computer Interaction with Mobile Devices and Services*, Glasgow, Scotland, 2004.

[70] Rovio, "Angry Birds," 2015. [Online]. Available: http://www.rovio.com/en/our-work/games/view/1/angry-birds. [Accessed February 2015].

[71] Booyah, "iTunes - MyTown2," 2015. [Online]. Available: https://itunes.apple.com/app/mytown-2/id442345455. [Accessed February 2015].

[72] E. Kaasinen, "User Needs for Location-Aware Mobile Services," *Personal and Ubiquitous Computing,* vol. 7, no. 1, pp. 70-79, May 2003.

[73] G. Disterer and C. Kleiner, "BYOD Bring Your Own Device," *Procedia Technology,* vol. 2013, no. 9, pp. 43-53, 2013.

[74] P. C. K. Hung, E. Ferrari and B. Carminati, "Towards Standardized Web Services Privacy Technologies," in *Proceedings of the IEEE International Conference on Web Services (ICWS'04)*, San Diego, CA, 2004.

[75] W3C, "Web Services Architecture," 2004. [Online]. Available: http://www.w3.org/TR/ws-arch. [Accessed 2014].

[76] W3C, "Web Services Description Language (WSDL) 1.1," W3C, 2001.

[77] J. Fonseca, Z. Abdelouahab, D. Lopes and S. Labidi, "A Security Framework for SOA Applications on Mobile Environment," *International Journal of Network Security & ITS Applications,* vol. 1, no. 3, pp. 90-107, 2009.

[78] Fusion Forge, "Welcome to the SOA4D Forge," [Online]. Available: https://forge.soa4d.org/. [Accessed September 2014].

[79] OASIS, "OASIS Devices Profile for Web Services," July 2009. [Online]. Available: http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01. [Accessed December 2013].

[80] Microsoft, "Intorducing Devices Profile for Web Services," 2007. [Online].

[81] R. Want, "An Introduction to RFID Technology," *IEEE Pervasive Computing,* vol. 5, no. 1, 2006.

[82] F. Golatowski, A. Bobek and E. Zeeb, "Web Services for Devices - About," WS4D, [Online]. Available: http://ws4d.e-technik.uni-rostock.de/about/. [Accessed September 2014].

[83] G. M. Araujo and F. Siqueira, "The Device Service Bus: A Solution for Embedded Device Integration through Web Services," in *Proceedings of the 2009 ACM Symposium on Applied Computing*, New York, NY, 2009.

[84] S. Pohlsen, S. Schlichting, M. Strahle, F. Franz and C. Werner, "A Concept for a Medical Device Plug-and-Play Architecture based on Web Services," *ACM SIGBED Review - Special Issue on the 2nd Joint Workshop on High Confidence Medical Devices, Software, and Systems (HCMDSS) and Medical Device Plug-and-Play (MD PnP) Interoperability,* vol. 6, no. 2, p. Article 6, 2009.

[85] C. El Kaed, Y. Denneulin and F.-G. Ottogalli, "Dynamic Service Adaptation for Plug and Play Device Interoperability," in *Proceedings of the 7th International Conference on Network and Services Management*, 2011.

[86] S. Unger, E. Zeeb, F. Golatowski, H. Grandy and D. Timmermann, "Extending the Devices Profile for Web Services for Secure Mobile Device Communication," in *4th International Workshop on Trustworthy Internet of People, Things & Services at the Internet of Things Conference*, Tokyo, Japan, 2010.

[87] P. C. K. Hung and V. S. Y. Cheng, "Privacy," in *Encyclopedia of Database Systems*, Springer, 2009, pp. 2136-2137.

[8 R. Sandhu and P. Samarati, "Access Control: Principles and Practice," *IEEE*
8] *Communications Magazine,* vol. 1994, no. September, pp. 40-48, 1994.

[8 Open Web Application Security Project (OWASP), "Access Control Cheat Sheet,"
9] OWASP, 2014.

[9 Hasbro, "Furby Boom," Hasbro, 2013.
0]

[9 A. H. Anderson, "A Comparison of Two Privacy Policy Languages: EPAL and XACML,"
1] in *Proceedings of the 3rd ACM Workshop on Secure Web Services*, New York, NY, 2006.

[9 W3C, "Extensible Markup Language (XML)," W3C, 2015.
2]

[9 R. Wenning, "Platform for Privacy Preferences (P3P) Project: Enabling Smarter Privacy
3] Tools for the Web," 20 November 2007. [Online]. Available: http://www.w3.org/P3P/. [Accessed December 2013].

[9 M. Olurin, C. Adams and L. Logrippo, "Platform for Privacy Preferences (P3P): Current
4] Status and Future Directions," in *2012 Tenth Annual International Conference on Privacy, Security and Trust (PST)*, Paris, France, 2012.

[9 WAP-W3C, "Report from WAP-W3C Joint Workshop on Mobile Web Privacy," W3C,
5] Munich, Germany, 2000.

[9 L. Cranor, "P3P is Dead, Long Live P3P!," 3 December 2012. [Online]. Available:
6] http://lorrie.cranor.org/blog/2012/12/03/p3p-is-dead-long-live-p3p/. [Accessed October 2013].

[9 L. Cranor, "Internet Explorer Privacy Protections also Being Circumvented by Facebook, and Many more," 18 February 2012. [Online]. Available:

7] http://www.techpolicy.com/Cranor_InternetExplorerPrivacyProtectionsBeingCircumvented-by-Google.aspx. [Accessed October 2013].

[98] J. Seligy and P. Lawson, "Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?," Canadian Internet Policy and Public Interest Clinic, Ottawa, 2006.

[99] P. Ashley, S. Hada, G. Karjoth, C. Powers and M. Schunter, "Enterprise Privacy Authorization Language (EPAL 1.2)," 10 November 2003. [Online]. Available: http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/. [Accessed March 2015].

[100] P. Ashley, S. Hada, G. Karjoth, C. Powers and M. Schunter, "The Enterprise Privacy Authorizsation Language (EPAL) - How to Enforce Privacy Throughout an Enterprise," 2003. [Online]. Available: http://www.w3.org/2003/p3p-ws/pp/ibm3.html. [Accessed March 2015].

[101] Open Geospatial Consortium, "GeoXACML," 15 December 2005. [Online]. Available: https://geoxacml.secure-dimensions.com/ . [Accessed December 2014].

[102] A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry and S. Waldbusser, "Terminology for Policy-Based Management," IETF RFC 3198, 2001.

[103] R. Yavatkar, D. Pendarakis and R. Guerin, "A Framework for Policy-Based Admission Control," IETF RFC2753, 2000.

[104] Open Systems Interconnection, *Information Technology - Security Frameworks for Open Systems: Access Control Framework,* 1966.

4]

[10 G. Waters, J. Wheeler, A. Westerinen, L. Rafalow and R. Moore, "Policy Framework Architecture," IETF, 1999.
5]

[10 World Wide Web Consirtium (W3C), "Web Services Architecture Requirements," 11 February 2004. [Online]. Available: http://www.w3.org/TR/wsa-reqs/.
6]

[10 D. Ferraiolo and R. Kuhn, "Role-based Access Control," in *Proceedings of the 15th National Computer Security Conference*, 1992.
7]

[10 Q. Ni, A. Trombetta, E. Bertino and J. Lobo, "Privacy-Aware Role Based Acces Control," in *SACMAT '07: Proceedings of the 12th ACM Symposium on Access Control Models and Technologies*, France, 2007.
8]

[10 J. Seifert, A. De Luca and B. Conradi, "A Context-Sensitive Security Model for Privacy Protection on Mobile Phones," in *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services*, New York, NY, 2009.
9]

[11 K. Ghazinour and K. Barker, "A Privacy Preserving Model Bridging Data Provider and Collector Preferences," in *Proceedings of the Joint EDBT/ICDT 2013 Workshops*, New York, NY, USA, 2013.
0]

[11 K. Ghazinour and K. Barker, "Capturing P3P Semantics Using and Enforceable Lattice-based Structure," in *Proceedings of the 4th International Workshop on Privacy and Anonymity in the Information Society*, New York, NY, USA, 2011.
1]

[1 S. Chakraborty, N. Bitouze, M. Srivastava and L. Dolocek, "Protecting Data Against

1 Unwanted Inferences," in *Proceedings of the 2013 IEEE Information Theory*
2] *Workshop*, Seville, Spain, 2013.

[1 A. Solanas, J. Domingo-Ferrer and A. Martinez-Balleste, "Location Privacy in Location-
1 Based Services: Beyond TTP-based Schemes," in *Privacy in Location-Based*
3] *Applications (PiLBA'08)*, Malaga, Spain, 2008.

[1 M. Duckham and L. Kulik, "A Formal Model of Obfuscation and Negotiation for
1 Location Privacy," in *Pervasive Computing*, vol. 3468, H. G. e. al., Ed., Munich,
4] Germany, Springer-Verlag Berlin Heidelberg, 2005, pp. 152-170.

[1 C. A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati and P. Samarati,
1 "Location Privacy Protection Through Obfuscation-based Techniques," in *Lecture*
5] *Notes in Computer Science: Data and Applications Security*, vol. 4602, Redondo
Beach, California: Springer Berlin Heidelberg, 2007, pp. 47-60.

[1 S. Taha and X. Shen, "A Physical-Layer Location Privacy-Preserving Scheme for Mobile
1 Public Hotspots in NEMO-Based VANETs," *IEEE Transactions on Intelligent*
6] *Transportation Systems,* vol. 14, no. 4, pp. 1665-1680, 2013.

[1 R. Cheng and S. Prabhakar, "Using Uncertainty to Provide Privacy-Preserving and
1 High-Quality Location-Based Services," in *Workshop on Location Systems Privacy and*
7] *Control (mobileHCI'04)*, Glasgow, Scotland, 2004.

[1 S. Merrill, N. Basalp, J. Biskup, E. Buchmann, C. Clifton, B. Kuijpers, W. Othman and E.
1 Savas, "Privacy Through Uncertainty in Location-Based Services," in *2013 IEEE 14th*
8] *International Conference on Mobile Data Management*, Milan, Italy, 2013.

[1 O. Jorns, O. Jung, J. Gross and S. Bessler, "A Privacy Enhancement Mechanism for
1 Location Based Service Architectures Using Transaction Pseudonyms," in *Lecture*
9] *Notes in Computer Science: Trust, Privacy, and Security in Digital Business*, vol. 3592,

Copenhagen, Denmark, Sprinter-Verlag Berlin Heidelberg, 2005, pp. 100-109.

[10] S.-H. Fang, W.-J. Lai and Y.-C. Liang, "An Encryption-Based Approach for Protecting Privacy in Network-Based Location Systems," in *IEEE 2011 International Conference on Machine Learning and Cybernetics (ICMLC)*, Guilin, 2011.

[11] M. Ashouri-Talouki and A. Baraani-Dastjerdi, "Homomorphic Encryption to Preserve Location Privacy," *International Journal of Security and Its Applications,* vol. 6, no. 4, pp. 183-190, 2012.

[12] B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," in *25th IEEE International Conference on Distributed Computing Systems*, Columbus, OH, 2005.

[13] D. Riboni, L. Pareschi and C. Bettini, "Privacy in Georeferenced Context-aware Services: A Survey," in *Privacy in Location-Based Applications (PiLBA'08)*, Malaga, Spain, 2008.

[14] R. Barnes, M. Lepinski, A. Cooper, J. Morris, H. Tschofenig and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications," IETF, 2011.

[15] J. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla and A. Murukan, "Chapter 3: Threat Modeling," in *Improving Web Application Security: Threats and Countermeasures*, Microsoft Corporation, 2003.

[16] S. Hernan, S. Lambert, T. Ostwald and A. Shostack, "Uncover Security Design Flaws Using the STRIDE Approach," MSDN Magazine, 2006.

[17] OWASP, "Application Threat Modeling," OWASP, 2013.

7]

[1 Open Web Application Security Project (OWASP), "OWASP Mobile Security Project -
2 Mobile Threat Model," February 2013. [Online]. Available:
8] https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Mobile_Threat_Model. [Accessed February 2015].

[1 S. Roosa, "Privacy Threat Model for Mobile," Center for Information Technology
2 Policy, 10 September 2012. [Online]. Available: https://freedom-to-
9] tinker.com/blog/sroosa/privacy-threat-model-for-mobile/. [Accessed February 2015].

[1 M. Deng, K. Wuyts, R. Scandariato, B. Preneel and W. Joosen, "A Privacy Threat
3 Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy
0] Requirements," in *Interdisciplinary Institute for Broadband Technology (IBBT)*, Belgium, 2010.

[1 M. Deng, K. Wuyts, R. Scandariato, B. Preneel and W. Joosen, "A Privacy Threat
3 Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy
1] Requirements," in *Interdisciplinary Institute for Broadband Technology (IBBT)*, Belgium, 2010.

[1 A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data
3 minimization: Anonymity, unlinkability, undetectability, unobservability,
2] pseudonymity, and identity management (v0.34 August 2010)," TU Dresden and ULD Kiel, 2010.

[1 A. Cooper, H. Tschofenig, B. Aboba, J. Peterson, J. Morris, M. Hansen and R. Smith,
3 "RFC 6973: Privacy Considerations for Internet Protocols," IETF, 2013.
3]

[1 United Nations Children's Fund (UNICEF), "Child Safety Online: Global Challenges and
3

4] Strategies," UNICEF, Florence, Italy, 2011.

[1 European NGO Alliance for Child Safety Online (eNASCO), "The Right Click: An Agenda
3 for Creating a Safer and Fairer Online Environment for Every Child," European NGO
5] Alliance for Child Safety Online, eNASCO, Copenhagen, 2010.

[1 A. F. Westin, Privacy and Freedom, New York: Athenum, 1967.
3
6]

[1 S. Chakraborty, K. Raghavan, M. Johnson and M. Srivastava, "A Framework for
3 Context-Aware Privacy of Sensor Data on Mobile Systems," in *The Fourteenth*
7] *Workshop on Mobile Computing Systems and Applications (ACM HotMobile 2013)*,
New York, USA, 2013.

[1 Toy Industry Association, "The Changing Privacy and Data Security Landscape - From
3 Mobile Apps to OBA," Keller and Heckman LLP, Washington, D.C., 2012.
8]

[1 M. Madden, S. Cortesi, U. Gasser, A. Lenhart and M. Duggan, "Parents, Teens, and
3 Online Privacy," Pew Research Center, Berkman Center for Internet & Society at
9] Harvard University, Washington D.C., 2012.

[1 European Union Safer Internet Program, "Benchmarking of Parental Control Tools for
4 the Onling Protection of Children," European Union Safer Internet Program.
0]

[1 E. Chin, A. P. Felt, V. Sekar and D. Wagner, "Measuring User Confidence in
4 Smartphone Security and Privacy," in *Symposium on Usable Privacy and Security*,
1] Washington, D.C., 2012.

[1 A. Felt, E. Ha, S. Egelman, A. Haney, E. Chin and D. Wagner, "Android Permissions:

4 User Attention, Comprehension, and Behavior," in *Symposium on Usable Privacy and*
2] *Security*, Washington, D.C., 2012.

[1 H. Peng, C. Gates, B. Sarma, N. Li, Y. Qi and R. Potharaju, "Using Probabilistic
4 Generative Models for Ranking Risks of Android Apps," in *ACM Conference on*
3] *Computer and Communications Security*, New York, 2012.

[1 Government of Canada, "Schedule 1 (Section 5) Principles Set out in the National
4 Standard of Canada Entitled Model Code for the Protection of Personal Information,"
4] *Personal Information Protection and Electronic Act (PIPEDA),* p. 20, 2000.

[1 Organization for Economic Cooperation and Development, "The OECD Privacy
4 Framework," 2013.
5]

[1 European Parliament and of the Council of the European Union, "Directive 95/46/EC
4 of the European Parliament and of the Council of 24 October 1995 on the protection
6] of individuals with regard to the processing of personal data and on the free
movement of such data," 24 October 1995. [Online].

[1 Health Canada, "Toys Regulations," Government of Canada, 2011.
4
7]

[1 MMA Privacy & Advocacy Committee, "Mobile Application Privacy Policy
4 Framework," Mobile Marketing Association, New York, London, Singapore, Sao Paulo,
8] 2011.

[1 CTIA - The Wireless Association, "Best Practices and Guidelines for Location Based
4 Services," CTIA, 2010.
9]

[150] Digital Advertising Alliance, "Application of Self-Regulatory Principles to the Mobile Environment," Digital Advertising Alliance, 2013.

[151] Q. He, "Privacy enforcement with an extended role-based access control model," NCSU Computer Science Technical Report TR-2003-09, February 2003.

[152] A. Rezgui, M. Ouzzani, A. Bouguettaya and B. Medjahed, "Preserving Privacy in Web Services," in *Proceedings of the Fourth International Workshop on Web Information and Data Manaagement*, 2002.

[153] F. Jammes, A. Mensch and H. Smit, "Service-Oriented Device Communications using the Devices Profile for Web Services," in *MPAC '05 Proceedings of the 3rd International Workshop on Middleware for Pervasive and Ad-Hoc Computing*, New York, NY, 2005.

[154] I. Luck, "JMEDS (Java Multi Edition DPWS Stack)," sourceforge.net, 2015.

[155] Sun Microsystems, "Sun's XACML Implementation," Sun Microsystems, 2006.

[156] Raspberry Pi Foundation, "Raspberry Pi 1 Model B+," Raspberry Pi Foundation, 2014.

[157] Y. Want, J. Wei and K. Vangury, "Bring Your Own Device Security Issues and Challenges," in *The 11th Annual IEEE Consumer Communications and Networking Conference (CCNC) - Mobile Device, Platform and Communication*, Las Vegas, NV,

7] 2014.

[1 P. C. K. Hung and V. S. Y. Cheng, "Privacy," in *Encyclopedia of Database Systems*,
5 Springer US, 2009, pp. 2136-2137.
8]

[1 R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec and J.-P. Hubaux, "Quantifying
5 Location Privacy," in *2011 IEEE Symposium on Security and Privacy*, 2011.
9]

[1 Health Canada, "Canada Consumer Product Safety Act," Government of Canada,
6 2010.
0]

[1 R. Shokri, J. Freudiger and J.-P. Hubaux, "A Unified Framework for Location Privacy,"
6 in *3rd Hot Topics in Privacy Enhancing Technologies*, 2010.
1]

[1 L. Cranor, Web Privacy with P3P, Sebastopol, CA: O'Reilly Media, Inc., 2002, p. 105.
6
2]

[1 W3C, "Web Services Policy 1.5 - Framework," W3C, 2007.
6
3]